UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"AUDITORÍA DE TI EN EL DEPARTAMENTO DE TALENTO HUMANO DEL GRUPO DE INTERVENCIÓN Y RESCATE DE LA POLICIA"

Trabajo de titulación previo a la obtención del título de Ingeniero en Tecnologías de la Información.

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética).

AUTOR:

Cristhian Daniel Chisaguano Chusete.

DIRECTOR:

Ing. Marco Remigio Pusdá Chulde, PhD.

Ibarra – Ecuador 2026.

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003561659		
APELLIDOS Y NOMBRES:	Chisaguano Chusete Cristhian Daniel		
DIRECCIÓN:	Pomasqui - Quito		
EMAIL:	cdchisaguanoc@utn.edu.ec		
TELÉFONO FIJO:	022 615 224	**TELÉFONO MÓVIL:**	0999560991

DATOS DE LA OBRA	
TÍTULO:	AUDITORÍA DE TI EN EL DEPARTAMENTO DE TALENTO HUMANO DEL GRUPO DE INTERVENCIÓN Y RESCATE DE LA POLICIA.
AUTOR (ES):	Cristhian Daniel Chisaguano Chusete.
FECHA: DD/MM/AAAA	04/03/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	[X] **PREGRADO** [ ] **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Tecnologías de la Información.
ASESOR /DIRECTOR:	Ing. Marco Remigio Pusdá Chulde, PhD.

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 04 días del mes de marzo de 2026

EL AUTOR:

Firmado electrónicamente por:
CRISTHIAN DANIEL CHISAGUANO CHUSETE
Validar únicamente con FirmaEC

.....
Cristhian Daniel Chisaguano Chusete.

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, a los 04 días del mes de marzo de 2026

Ing. Marco Remigio Pusdá Chulde, PhD.
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR
CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

MARCO REMIGIO PUSDA CHULDE

Firmado digitalmente por MARCO REMIGIO PUSDA CHULDE
Fecha: 2026.03.04 15:41:37 -05'00'

Ing. Marco Remigio Pusdá Chulde, PhD.

C.C: 040120095-1

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificador del trabajo de Integración Curricular " "AUDITORIA DE TI EN EL DEPARTAMENTO DE TALENTO HUMANO DEL GRUPO DE INTERVENCION Y RESCATE DE LA POLICIA" " elaborado por Cristhian Daniel Chisaguano Chusete , previo a la obtención del título del Ingeniero en Tecnologías de la Información , aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

MARCO REMIGIO PUSDA CHULDE

Firmado digitalmente por MARCO REMIGIO PUSDA CHULDE
Fecha: 2026.03.04 15:42:01 -05'00'

Ing. Marco Remigio Pusdá Chulde, PhD.

C.C: 040120095-1

Firmado electrónicamente por:
DAISY ELIZABETH IMBAQUINGO ESPARZA
Validar únicamente con FirmaEC

Ing. Daisy Elizabeth Imbaquingo Esparza, PhD.

C.C: 100287304-8

DEDICATORIA

Este logro académico representa mucho más que la culminación de un ciclo de estudios, es el fruto de una fe inquebrantable, del apoyo incondicional y del amor de quienes han caminado a mi lado. En primer lugar, elevo mi más sincero agradecimiento a Dios por ser mi guía, mi fortaleza y la luz que ilumina cada paso de este camino. A él dedico el esfuerzo y la perseverancia puestos en esta obra. Con todo mi corazón, dedico este trabajo a mi familia, mi pilar fundamental. A ti, padre Manuel Chisaguano, por tu ejemplo de constancia y trabajo duro, por enseñarme que la integridad es el valor más alto. A ti, madre Laura Chusete, por tu amor inagotable, por tus oraciones que me sostuvieron en los momentos más complejos y por creer en mí incluso cuando yo dudaba. A mis hermanos, mis compañeros de vida, Liliana, Nancy, Bryan y Yajaira. Gracias por cada palabra de aliento, por la complicidad y la alegría que han llenado nuestro hogar. Este título también es suyo, porque cada meta alcanzada se comparte con quienes se alegran genuinamente por los triunfos propios.

Que estas páginas sean un testimonio de que, con fe, unidad familiar y determinación, los sueños se convierten en realidad. Esta victoria es de todos nosotros.

Con todo mi amor y gratitud.

Cristhian Daniel Chisaguano Chusete

AGRADECIMIENTO

La realización de este trabajo de titulación no hubiera sido posible sin el invaluable apoyo y la colaboración de muchas personas a quienes deseo expresar mi más profundo reconocimiento. Mi primer y más sincero agradecimiento es para Dios, fuente de sabiduría y fortaleza. Su guía divina fue mi faro en los momentos de mayor desafío intelectual y personal, recordándome que toda capacidad y todo logro provienen de Él. A mi querida familia, mi más sólido fundamento. A mis padres, Manuel Chisaguano y Laura Chusete, les agradezco infinitamente su sacrificio silencioso, su apoyo incondicional y su fe inquebrantable en mi potencial. Ustedes han sido el motor de este logro. A mis hermanos, Liliana, Nancy, Bryan y Yajaira, por su constante alegría, su paciencia durante mis ausencias y por ser mi refugio de complicidad y ánimo inagotable. Este título lleva sus nombres. Extiendo mi gratitud a todos aquellos que, de una u otra forma, contribuyeron a este camino. A mis profesores y tutores, por compartir su conocimiento y brindar su orientación experta. A mis compañeros de estudio, por el intercambio de ideas, el mutuo apoyo y por su invaluable asistencia.

A cada persona que me tendió una mano, me dio un consejo o simplemente creyó en mí: muchas gracias. Este logro es colectivo, tejido con el apoyo de una comunidad que crece y aprende junta.

Con eterna gratitud.

Cristhian Daniel Chisaguano Chusete

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este estudio tuvo como objetivo validar una propuesta de mejora para la seguridad de TI en procesos de reclutamiento del Grupo de Intervención y Rescate (GIR) de la Policía Nacional del Ecuador, unidad élite especializada en operaciones de alto riesgo como liberación de secuestrados y neutralización de objetivos de alto valor, con el método Delphi, siete expertos en seguridad informática evaluaron 36 controles basados en COBIT 2019, viendo su nivel de madurez y aplicabilidad Utilizando el método Delphi, siete expertos en seguridad informática evaluaron 36 controles basados en COBIT 2019, analizando tanto su nivel de madurez como su aplicabilidad en el contexto operativo del GIR. En un primer momento, la ronda inicial mostró un acuerdo con una concordancia aceptable (W = 0.36), identificándose ocho controles con alta variabilidad (CV >0.35). Esto evidenció diferencias claras en los puntos de vista de los expertos respecto a la implementación de controles técnicos y organizativos, posteriormente, tras una segunda ronda de retroalimentación estructurada, que incluyó estadísticos descriptivos y análisis de consenso, se alcanzó un acuerdo unánime (W = 1.00), junto con una valoración alta en todos los controles, lo que permitió demostrar la viabilidad y relevancia de las medidas propuestas, en consecuencia, el plan planteado tiene como propósito socializarse con los miembros del GIR para su aplicación práctica, con el fin de asegurar los datos de los aspirantes y optimizar los procesos de reclutamiento futuros, la metodología empleada confirmó su eficacia para consolidar criterios expertos y generar propuestas técnicamente sólidas, contribuyendo a la protección de información sensible en contextos operativos críticos, donde la confidencialidad e integridad de los datos resultan prioritarias para el cumplimiento de la misión institucional.

Palabras clave: Método Delphi, COBIT 2019, seguridad TI, consenso de expertos, controles de seguridad, GIR.

ABSTRACT

This study aimed to validate a proposed improvement to IT security in the recruitment processes of the Intervention and Rescue Group (GIR) of the Ecuadorian National Police, an elite unit specializing in high-risk operations such as hostage rescue and the neutralization of high-value targets. Using the Delphi method, seven IT security and governance experts evaluated 36 controls based on COBIT 2019, measuring their maturity level and applicability within the GIR's operational context. The first round showed acceptable agreement ($W = 0.36$; $p < 0.001$), identifying eight controls with high variability (CV >0.35) that reflected differences in the experts' perceptions regarding the implementation of technical and organizational controls. After a second round of structured feedback, which included descriptive statistics and consensus analysis, unanimous agreement was achieved ($W = 1.00$) and a high rating across all controls, demonstrating the viability and relevance of the proposed measures. The resulting plan is intended to be shared with GIR members for practical application, in order to safeguard applicant data and optimize future recruitment processes. The methodology employed proved effective in consolidating expert criteria and generating technically robust proposals, contributing to the protection of sensitive information in critical operational contexts where data confidentiality and integrity are paramount for fulfilling the institutional mission.

Keywords: Delphi method, COBIT 2019, IT security, expert consensus, security controls, GIR.

CAPÍTULO I
INTRODUCCIÓN

1.1 Planteamiento del Problema.

El GIR gestiona una gran cantidad de información delicada, datos que no solo afectan al equipo humano, sino también a la administración operativa de la seguridad nacional, esta información incluyendo datos personales y estrategias clave, es esencial para mantener la protección y el funcionamiento de la institución, sin embargo, uno de los grandes desafíos que enfrenta la entidad es la mala gestión con sistemas informáticos para la administración de su talento humano (miembros altamente capacitados en misiones de alto riesgo en seguridad nacional) debido a la escasez de recursos.

Esa posible mala gestión ha permitido lamentablemente un retraso en la ejecución de operativos planificados y de emergencia lo que representa una vulnerabilidad enorme en la seguridad nacional [1], el GIR en su papel de entidad de élite responsable de la seguridad nacional, se encuentra con graves inquietudes vinculadas con la gestión de datos delicados y reservados que gestiona en su departamento de recursos humanos, actualmente existe una falta de auditoría sistemática de los sistemas informáticos, lo que provoca vulnerabilidades en la protección de datos críticos, así como ineficiencias en los procesos administrativos [2].

Esto plantea la pregunta: ¿qué está pasando? Las causas de este problema incluyen la ausencia de políticas de seguridad informática, la falta de capacitación del personal en el uso de herramientas tecnológicas adecuadas para el manejo de la información [3], estas deficiencias generan consecuencias considerables, incluyendo la potencial evasión de información delicada, lo cual pone en riesgo la integridad de las operaciones y la identidad de los miembros del colectivo, esto puede estar afectando la capacidad de respuesta ante situaciones críticas.

Las variables involucradas en este proceso fueron la calidad de los sistemas informáticos, el nivel de capacitación del personal, las políticas de seguridad implementadas y la infraestructura tecnológica disponible, dentro del campo de la ingeniería en tecnologías de la información, este problema podría ser abordado mediante una auditoría meticulosa de los sistemas existentes, identificando vulnerabilidades y proponiendo mejoras pertinentes.

El objetivo fue concebir e implementar protocolos de seguridad que aseguren la integridad y confidencialidad de la información, junto con la formación de personal para optimizar la utilización de las herramientas digitales, esta perspectiva holística no solo optimizó los procesos administrativos, sino que también robustecerá la seguridad nacional, salvaguardando la información crítica de la institución, de los funcionarios públicos y de la sociedad ecuatoriana. ”Las auditorías se llevan a cabo con el objetivo de evaluar la conformidad de una organización con los procedimientos estándar e identificar oportunidades de mejora”[4].

1.2 Objetivos.

1.2.1 Objetivo General.

Realizar una auditoría de tecnologías de la información (TI) en el departamento de talento humano del Grupo de Intervención y Rescate de la Policía Nacional del Ecuador en base al estándar COBIT 2019.

1.2.2 Objetivos Específicos.

- Realizar un levantamiento de información acerca de los sistemas informáticos actuales utilizados en el departamento de talento humano.

- Realizar una propuesta para el proceso de reclutamiento en base a COBIT 2019 con la finalidad de que cumpla estándares de seguridad.

- Evaluar la propuesta de mejora para el proceso de reclutamiento en el Grupo de Intervención y Rescate.

1.3 Alcance y delimitación.

Esta investigación denominada, auditoría TI en el departamento de talento humano del Grupo de Intervención y Rescate de la Policía Nacional del Ecuador, se enfocó en una evaluación meticulosa de los sistemas informáticos y las políticas de seguridad de la información implementadas en la administración del capital humano de una de las unidades elite de la Policía Nacional del Ecuador, situada en Quito, Ecuador, sector Pusuquí, la cual realizó un levantamiento de información con métodos directos, en base a las metas y a los objetivos del estándar COBIT 2019 determinados, además se verificó el control de accesos a la información, cuantas personas que tienen acceso al departamento de talento humano [5].

Se realizó una propuesta que se aplique en el proceso de reclutamiento en base a COBIT 2019 con la finalidad de que cumpla estándares de seguridad, se propuso aplicar los principios de gobierno y gestión de TI de COBIT 2019 de manera específica.

Se estableció un marco de gobierno que defina roles y responsabilidades claras en el proceso de reclutamiento, asegurando que se cumplan los principios de satisfacer las necesidades de las partes interesadas y cobertura integral del departamento de talento humano del Grupo de Intervención y Rescate de la Policía Nacional del Ecuador, esto implica asegurar que sus necesidades y expectativas sean consideradas [6].

Se implementó una propuesta de plan de mejora con un enfoque holístico para la gestión de riesgos, con el principio de aplicación de un enfoque único e integrado, que permitió identificar, evaluar y mitigar los riesgos asociados con la seguridad de la información durante el reclutamiento, por último se utilizó herramientas y tecnologías que cumplen con los estándares de seguridad de la información, alineándose con el principio de habilitación de un enfoque sistémico, para garantizar la integridad, confidencialidad y disponibilidad de los datos de los candidatos en todo el proceso, mediante un análisis de costo beneficio.

Dado que el talento humano que forma parte de este grupo de élite tiene competencia a nivel nacional, la auditoría aborda no sólo los procesos administrativos locales, sino también su impacto en las operaciones que se realizan en las diferentes regiones del país, esto permitió identificar vulnerabilidades y proponer soluciones que beneficien a todos los empleados, garantizando que la gestión de la información sensible sea eficiente y segura [7].

La investigación se centró en analizar los sistemas actuales, identificar vulnerabilidades en las políticas de seguridad, formular recomendaciones y capacitar al personal, los resultados de esta auditoría no sólo hicieron un diagnóstico certero de la situación actual, sino que también ofreció un camino claro para implementar mejoras sostenibles, promoviendo un ambiente de confianza y seguridad.

1.4 Justificación.

La auditoría fué realizada mediante la metodología Delphi que constituye una necesidad urgente y tiene un impacto directo en la seguridad y la eficacia de los procedimientos policiales.

Aportó una mayor seguridad en los sistemas informáticos del departamento de talento humano del Grupo de Intervención y Rescate, mejorando así la protección de la información confidencial y estratégica, en un contexto global donde la información representa uno de los activos más valiosos, asegurar la salvaguarda de datos confidenciales se erige como una obligación

crítica, particularmente para una unidad encargada de la gestión de información de naturaleza confidencial y estratégica.

Es imperativo admitir que el Grupo de Intervención y Rescate desempeña un papel fundamental en la seguridad pública de Ecuador, sus integrantes no solo asumen la responsabilidad de llevar a cabo operaciones de rescate e intervención en circunstancias de emergencia o alto riesgo, sino también de administrar información crítica vinculada a sus operaciones y personal, la administración eficaz del capital humano constituye un elemento fundamental para el éxito de dichas operaciones y la seguridad pública.

En caso de vulnerabilidad de los sistemas informáticos que respaldan esta administración, no solo se encuentra en peligro la identidad y la seguridad de los agentes, sino también la seguridad de los ciudadanos a los que prestan servicios, este estudio tiene como objetivo también establecer la respectiva relevancia de capacitación continua de los individuos en el manejo de las tecnologías de la información.

La formación en terreno se enfoco utilizando herramientas, que abarcaron sensibilización sobre la seguridad de la información y las prácticas óptimas para su protección, un equipo altamente cualificado constituye un recurso inestimable que tiene la capacidad de identificar y atenuar los riesgos antes de que se materialicen en problemas de gravedad [8], dentro de este marco, la auditoría emerge como un instrumento para identificar áreas de mejora en la capacitación personal, asegurando que cada miembro esté debidamente formado para contribuir a un ambiente más seguro.

La implementación de una auditoría a los procesos de reclutamiento del Grupo de Intervención y Rescate de la Policía Nacional del Ecuador contribuyó al fortalecimiento de la administración de recursos humanos y a la instauración de una cultura de seguridad dentro de la institución, asimismo, permitió la instauración de protocolos de seguridad que sean adaptables a las amenazas emergentes [9], el compromiso con esta investigación va más allá del cumplimiento de un requisito académico, es un llamado a la acción una oportunidad para contribuir al bienestar de la sociedad y la seguridad nacional, al abordar las vulnerabilidades en los sistemas de TI, estamos influyendo en la seguridad pública del Ecuador, esta auditoría de campo aplicada al grupo GIR, más que resolver buscó identificar problemas de vulnerabilidades en los sistemas de TI del Departamento de Talento Humano, que ponen en riesgo tanto la seguridad de los agentes como la efectividad de los operativos policiales, pero además fue un agente de cambio que promovió la

confianza en los procesos administrativos, mejorando así la calidad del servicio brindado a los ciudadanos.

En un mundo progresivamente digital, la seguridad informática ha emergido como un asunto de considerable importancia, las amenazas cibernéticas son constantes y evolucionan rápidamente, lo que significa que las instituciones deben estar siempre un paso por delante, la auditoría aporta beneficios técnicos en términos de establecimiento de protocolos de seguridad informática y adaptabilidad a amenazas cibernéticas emergentes, esto no sólo protege la información, sino que también ayuda a construir una cultura de seguridad dentro de la institución [10].

Esta auditoria proporcionó conocimientos prácticos en relación con la ejecución de auditorías informáticas, la administración de riesgos en sistemas de información de carácter confidencial y la formación del personal en prácticas de seguridad de la información, el enfoque de la cascada de metas propuesto por COBIT 2019 se emplea para transformar las necesidades de los actores interesados en una estrategia corporativa viable.

Estas necesidades generaron un impacto en cascada sobre los objetivos corporativos o empresariales (EG#), los cuales a su vez influyen en los objetivos de alineación o metas vinculadas a las tecnologías de la información (AG#), posteriormente, estos ejercieron un impacto en cascada sobre los objetivos de gobernanza y gestión [11], que deben implementarse en el ámbito corporativo, todo este proceso se alineó con la lógica de la cascada de metas, tal como se observa en la Fig. 1.

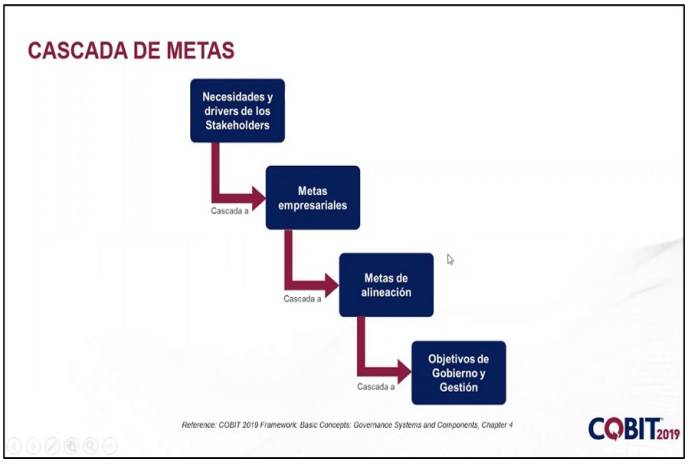

Fig. 1. Cascada de metas propuesta por COBIT 2019 [11]

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes.

El 22 de octubre de 2021, la oficina central de la ANT en Quito fue objeto de incursiones por parte de la fiscalía y la policía, el objetivo era obtener datos e identificar a los autores de un incidente (ataque informático), la fiscalía inició una investigación por este caso debido al presunto delito de ataque a la integridad del sistema informático, durante el allanamiento los agentes se llevaron dos teléfonos y tres discos duros de los funcionarios de la ANT.

La entidad afirmó en un comunicado que esta vulnerabilidad del sistema informático impedía a los usuarios realizar los trámites de licencia y registro de automóviles [12], la Policía Nacional comunicó que se había producido erróneamente una alerta de detención contra Juan Carlos I. debido al uso no consentido de un usuario del servidor policial. JC fue compañero sentimental de la modelo Noemí Arcentales, cuya muerte se descubrió en Manta, Manabí, el 12 de diciembre de 2021, se trataba de un ex fiscal.

En un anuncio divulgado la tarde del miércoles 29 de diciembre de 2021, la entidad confirmó la presunta utilización indebida del usuario de un servidor policial asignado al subsistema investigativo en el sistema informático integral de la Policía Nacional del Ecuador (SIIPNE 3W) mediante el análisis de pistas de auditoría [13], un inquietante aumento de la frecuencia y sofisticación de los intentos de ingeniería social se puso de manifiesto en un estudio realizado en Ecuador en el 2022, se examinaron cualitativamente informes y datos, los resultados mostraron un desconocimiento general.

La necesidad de los planes preventivos y de respuesta eficaces para estos riesgos crecientes en Ecuador, en el 2022 se documentaron pagos a ciberdelincuentes por un total de más de 7,8 millones de dólares [14], en el 2023 el Ecuador ha experimentado un preocupante aumento de los ciberataques en los últimos años, y el país destaca en el Eset Security Report Latam 2023 por tener el mayor porcentaje de detecciones de phishing (8 %) de la zona, según una encuesta, los ciberataques son cada vez más rentables y dirigidos, lo que enfatiza la urgente necesidad de que instituciones clave como el Grupo de Intervención y Rescate de la Policía Nacional del Ecuador fortalezcan su ciberseguridad.

Según la investigación de Kaspersky, Ecuador registró 212.000 ataques en 2023, siendo el ransomware WannaCry el más común, esto pone de manifiesto la susceptibilidad de los sistemas

informáticos y enfatiza la necesidad de realizar auditorías informáticas para salvaguardar los datos confidenciales y mejorar la gestión de los recursos humanos [15].

2.2 Bases teóricas.

2.2.1 Cobit 2019.

Representa un marco de gobernanza y administración de tecnologías de la información (TI) que ofrece un enfoque holístico para la administración de la información y la tecnología en las organizaciones, este marco se fundamenta en las prácticas óptimas y estándares internacionales, facilitando a las organizaciones la alineación de sus metas de TI con las metas corporativas COBIT 2019, se ajusta a las demandas fluctuantes de las organizaciones, simplificando la implementación de controles y la administración de riesgos en un contexto digital en perpetua transformación [16].

Una de las características más destacadas de COBIT 2019 es su enfoque en la creación de valor a través de la gestión de TI, este marco no solo se centra en la seguridad y el cumplimiento, sino que también busca maximizar el valor de las inversiones en tecnología [17], este objetivo se alcanza a través de la detección de oportunidades de mejora y la optimización de los recursos tecnológicos existentes, lo cual conduce a un incremento en la eficiencia operativa y un mejor rendimiento organizacional.

La flexibilidad de cobit 2019 es otra de sus ventajas, este marco se puede adaptar a diferentes contextos organizacionales, independientemente del tamaño o la industria, esto significa que las organizaciones pueden personalizar la implementación de cobit 2019 según sus necesidades específicas, lo que facilita su adopción y maximiza su efectividad en la gestión de TI. Esta adaptabilidad es crucial en un entorno empresarial donde las tecnologías y los riesgos evolucionan rápidamente [18].

Cobit 2019 fomenta la integración de la gobernanza de tecnologías de la información con la gobernanza corporativa, esta integración es crucial para asegurar que las decisiones vinculadas a la tecnología se encuentren en consonancia con los objetivos estratégicos de la entidad [19], al establecer un vínculo explícito entre la gobernanza de tecnologías de la información y la gobernanza corporativa, las entidades pueden optimizar el proceso de toma de decisiones y garantizar que las inversiones en tecnología generen un valor tangible para la empresa.

La puesta en marcha de cobit 2019 también conlleva la adopción de un enfoque basado en riesgos, que posibilita a las organizaciones la identificación, evaluación y mitigación de los riesgos vinculados al empleo de la tecnología [20], mediante el enfoque en la administración de riesgos, las entidades pueden salvaguardar sus activos de información y asegurar la continuidad empresarial, un aspecto particularmente relevante en un contexto donde las amenazas cibernéticas se presentan con creciente frecuencia y sofisticación.

Otro aspecto relevante de cobit 2019 es su énfasis en la mejora continua, el marco fomenta la revisión y actualización periódica de los procesos de TI [21], esto posibilita que las organizaciones se ajusten a las fluctuaciones en el contexto empresarial y tecnológico, esta cultura de mejora continua es esencial para preservar la pertinencia y eficacia de la administración de tecnologías de la información, garantizando que las organizaciones puedan responder de manera ágil a las emergentes demandas y retos.

La formación y el fomento de habilidades en el personal constituyen componentes esenciales para la implementación exitosa de cobit 2019, es esencial que los expertos en tecnologías de la información posean un entendimiento profundo de los principios y prácticas de cobit para su aplicación efectiva en sus organizaciones, la instrucción continua y el perfeccionamiento de competencias son fundamentales para asegurar que el personal esté capacitado para afrontar los retos inherentes a la administración de tecnologías de la información y aportar al cumplimiento de los objetivos organizacionales [22].

Este marco COBIT 2019 se presenta como un marco robusto y flexible que en consecuencia permite a las empresas gestionar eficazmente sus recursos tecnológicos con un enfoque en la creación de valor,de manera semejante la integración en el gobierno corporativo y la gestión de riesgos, es una herramienta valiosa para las empresas que buscan optimizar su gobierno de TI.

Mediante la implementación de cobit 2019, las entidades pueden optimizar su adaptabilidad a un ambiente empresarial en constante evolución y asegurar que sus inversiones en tecnología produzcan resultados positivos y sostenibles, cobit 2019, ya tenido varios cambios a razón de cobit 5 como podemos ver en la Fig. 2 [11].

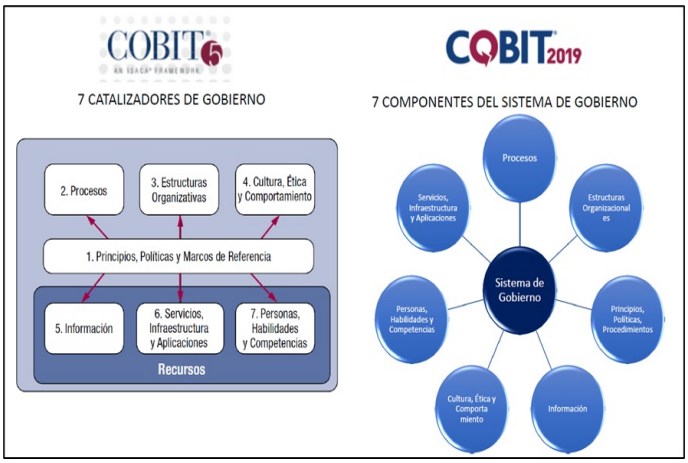

Fig. 2. Cobit 5 vs Cobit 2019 [11]

Según el informe de ESET (2024)[23], las tendencias en ciberseguridad para 2025 estarán marcadas por el aumento del uso malicioso de la inteligencia artificial generativa, el fortalecimiento de la protección de los sistemas OT (Tecnología Operativa) en infraestructuras críticas y la necesidad de marcos legales y éticos más sólidos que regulen el uso de la IA, aspectos esenciales para garantizar la seguridad y la integridad de los sistemas informáticos institucionales. La ley orgánica de protección de datos personales (2021)[24] del Ecuador establece un marco normativo orientado a garantizar el derecho a la privacidad, seguridad y tratamiento legítimo de la información personal, su aplicación implica la implementación de medidas técnicas, organizativas y legales que aseguren la confidencialidad, disponibilidad e integridad de los datos, en auditorías de TI como las realizadas en instituciones públicas, esta ley resulta esencial para evaluar el cumplimiento normativo y la gestión responsable de los datos personales.

En relación a la auditoría de TI para organismos de seguridad, es fundamental considerar la creciente sofisticación de las ciberamenazas. Kaspersky (2025)[25] reporta que, aunque las detecciones de ransomware masivo disminuyeron en 2024, los ataques selectivos a organizaciones de alto valor, como agencias gubernamentales, aumentaron significativamente, representando el 41.6 % de los incidentes atendidos por su equipo de respuesta, estos grupos emplean tácticas avanzadas como la doble extorsión y el modelo ransomware como servicio (RaaS), lo que exige que los marcos de gobierno como cobit 2019 se implementen con rigurosidad para proteger datos sensibles, como los del talento humano en una unidad policial de élite (GIR).

2.2.2 Auditoria de la seguridad de la información.

Se trata de un procedimiento esencial para garantizar una protección adecuada de los sistemas y datos de una organización, este procedimiento examina la efectividad de los controles de

seguridad, detecta vulnerabilidades y verifica la adhesión a las regulaciones vigentes, el propósito primordial es asegurar que las estrategias implementadas sean adecuadas para la mitigación de riesgos, particularmente en un contexto donde las amenazas cibernéticas se presentan con creciente frecuencia y complejidad [26].

Uno de los fundamentos de la auditoría de seguridad radica en garantizar la confidencialidad, integridad y disponibilidad de la información, estos tres principios, denominados la tríada CIA, son fundamentales para la protección de datos de naturaleza delicada, la auditoría posibilita la identificación de deficiencias en los protocolos de seguridad y la propuesta de medidas correctivas, lo cual robustece la salvaguarda de la información y disminuye la probabilidad de brechas de seguridad [27].

El enfoque metodológico de una auditoría de seguridad comúnmente comprende la evaluación de políticas, procedimientos y controles técnicos, también se llevan a cabo evaluaciones de penetración y pruebas de vulnerabilidades con el objetivo de identificar vulnerabilidades en los sistemas, estas evaluaciones simulan potenciales ataques, facilitando así la evaluación de la eficacia de las estrategias de defensa y una mejor preparación frente a amenazas cibernéticas [28].

El cumplimiento de normativas y estándares es un aspecto crítico en la auditoría de seguridad, las organizaciones deben alinearse con regulaciones como el GDPR, ISO 27001 y otras específicas de su sector, la auditoría verifica que se cumplan estos requisitos y señala áreas de mejora, lo que aumenta la confianza de los stakeholders [19], gestión de riesgos es un componente central en la auditoría de seguridad, este proceso implica identificar, evaluar y priorizar riesgos asociados a la información[29].

Al analizar amenazas potenciales y vulnerabilidades existentes, las organizaciones pueden implementar medidas correctivas y asignar recursos de manera eficiente, lo que es vital para mantener la seguridad de los activos informáticos [30], la cultura de seguridad dentro de una organización es otro aspecto evaluado en una auditoría, la concienciación y capacitación del personal son fundamentales para prevenir incidentes de seguridad, la auditoría puede detectar deficiencias en la formación del equipo y recomendar programas de capacitación, lo que reduce el riesgo de errores humanos que puedan comprometer la información [31].

Los informes deben ser claros y detallados, destacando las vulnerabilidades encontradas y las acciones recomendadas, estos documentos son herramientas clave para la toma de decisiones y la priorización de inversiones en seguridad [5], la auditoría de seguridad no es un evento

único, sino un proceso continuo, las organizaciones deben programar auditorías periódicas para adaptarse a los cambios en el entorno de amenazas [32].

La implementación de marcos de auditoría, tales como cobit 2019, optimiza la eficacia del proceso, cobit proporciona un enfoque estructurado para la gobernanza y administración de tecnologías de la información, facilitando así la detección de riesgos y la instauración de controles, mediante la adhesión a un marco reconocido, las entidades pueden garantizar que sus auditorías se encuentren en consonancia con las prácticas óptimas a nivel internacional [33].

La auditoría de seguridad promueve también la mejora continua de los procesos, los resultados obtenidos deben ser aplicados para la modificación de políticas y procedimientos, permitiendo a las organizaciones adaptarse a amenazas emergentes y optimizar su estrategia de seguridad, este enfoque proactivo es fundamental para preservar la confianza de los clientes y las partes interesadas [34].

2.2.3 Auditoría informática.

La auditoría informática constituye un procedimiento crucial que posibilita a las entidades evaluar la eficacia de sus sistemas de información y mecanismos de control de seguridad [35], la metodología utilizada en las auditorías informáticas puede variar, pero generalmente incluye la revisión de políticas, procedimientos y controles técnicos, es importante realizar pruebas para identificar debilidades en los sistemas, estas pruebas permiten a las organizaciones simular ataques y evaluar la efectividad de sus defensas.

Se considera documental porque se fundamenta en el análisis de normas, estándares internacionales (COBIT 2019, ISO/IEC 27001, NIST CSF) y literatura científica relacionada con la auditoría de seguridad informática y la gobernanza de TI, a su vez, es de campo, ya que se aplicaron encuestas, directamente en el contexto del GIR, obteniendo información primaria sobre la situación real de los sistemas y procesos auditados.

La auditoría informática debe considerar el cumplimiento de normativas y estándares relevantes, la auditoría ayuda a verificar que se cumplan estos requisitos y a identificar áreas donde se necesiten mejoras, la administración de riesgos debe enfocarse en la detección y valoración de riesgos vinculados a la información, lo que significa examinar las posibles amenazas y las debilidades presentes, además de valorar el efecto que podrían generar en la organización.

La administración de riesgos facilita la priorización de las acciones correctivas y la distribución eficaz de recursos, lo cual es crucial para preservar la seguridad de la información [36], el proceso de auditoría informática debería incorporar también la evaluación de la cultura de seguridad dentro de la organización, esta auditoría puede contribuir a identificar insuficiencias en la capacitación del personal y sugerir programas de formación para optimizar la cultura de seguridad, esto, a su vez, disminuye la probabilidad de incidentes de seguridad ocasionados por errores humanos [37].

Esta capacidad permite a las entidades adaptarse a las fluctuaciones en el contexto de amenazas y garantizar la eficacia de sus protocolos de seguridad, un aspecto esencial en un mundo donde las amenazas cibernéticas están en constante evolución, la auditoría informática también puede contribuir a la mejora continua de los procesos de seguridad, los hallazgos deben ser utilizados para ajustar y mejorar las políticas y procedimientos de seguridad [38].

La auditoría de sistemas constituye un proceso fundamental que permite a las organizaciones evaluar la eficacia de sus sistemas de información y sistemas de seguridad, a través de la identificación de vulnerabilidades, la gestión de riesgos y la observancia de normativas, las auditorías de seguridad informática asisten a las organizaciones en la optimización de su posición de seguridad y en la protección de sus recursos de información [39], para entender también es importante hacer una comparación entre auditoria informática y auditoria de la seguridad de la información [40], como se presenta en la Tabla 1 .

Tabla 1.
COMPARATIVA: AUDITORÍA INFORMÁTICA VS AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN

Aspecto	**Auditoría Informática**	**Auditoría de la Seguridad de la Información**
¿En qué consiste?	Es como un chequeo completo a todo el ecosistema tecnológico: sistemas, infraestructura y cómo se hacen las cosas.	Se mete de lleno con los controles y las barreras que protegen la información.

Aspecto	Auditoría Informática	Auditoría de la Seguridad de la Información
La meta principal	Ver que todo funcione como debería, que sea eficiente y que cumpla con la normativa.	Asegurarse de que los datos estén a salvo, sean correctos y estén disponibles cuando hagan falta.
Qué cubre?	En definitiva tiene un alcance bastante amplio el hardware, el software, las redes, las bases de datos.	Es más concreto; se enfoca en los datos y los activos de información, que son el corazón del asunto.
Zonas que revisa	La infraestructura tecnológica, el software que usan, el estado de las redes y cómo están montadas las bases de datos.	En sintesis, los controles de acceso quién entra y dónde, las políticas de seguridad, conviene resaltar que se gestionan los riesgos y el plan para cuando las cosas salen mal.
Normas que sigue	COBIT, ISO/IEC 27001, ITIL y, por supuesto, la legislación local de turno.	Se guía por la ISO/IEC 27001, la 27002 y el marco del NIST, que son como sus biblias.
Herramientas del oficio	Software para analizar sistemas, herramientas para vigilar la red y pruebas para medir el rendimiento.	se utilizará detectores de vulnerabilidades,también, se realizará escáneres de seguridad y sistemas SIEM que centralizan todos los logs.
Qué se espera lograr?	Encontrar los puntos flacos en los sistemas, mejorar su eficiencia y que no haya problemas con la ley.	De este modo queremos obtener vulnerabilidades y blindar la protección de la información y que los riesgos bajen de nivel.

Las auditorías de sistemas abarcan varios tipos, cada uno centrado en áreas específicas para garantizar la seguridad y la eficiencia de los sistemas. Las auditorías forenses se encargan

de investigar incidentes de ciberseguridad y recuperar datos comprometidos, mientras que las auditorías web evalúan la seguridad y la funcionalidad de sitios web y aplicaciones en línea.

La auditoría de código examina el software con el objetivo de identificar fallos o vulnerabilidades presentes en su codificación, en última instancia, la auditoría física corrobora la salvaguarda de instalaciones y hardware frente a intrusiones no autorizada en conjunto [41], estas auditorías contribuyen al fortalecimiento de la integridad en los contextos tecnológicos, así también podemos ver más ejemplos en la Fig. 3.

Fig. 3. Tipos de Auditorías Informáticas. [11]

2.2.4 Trabajos relacionados.

Millennials y generación X frente a la realidad del Big Data y la protección de datos personales en internet, Herrera y Guerrero en su investigación, subraya la creciente inquietud entre los ciudadanos respecto a la salvaguarda de sus datos personales en el marco del Big Data, esta investigación resulta relevante para nuestra auditoría informática, dado que proporciona un marco teórico que subraya la relevancia de instaurar protocolos de seguridad que protejan la información delicada.

En el contexto del grupo especial de la policía nacional del Ecuador, la salvaguarda de la información no solo es esencial para la protección de su privacidad, sino también para preservar la confianza pública en la administración de información crítica [42] , impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones, este estudio examina la relevancia de la auditoría informática como instrumento esencial para la salvaguarda de datos personales en agrupaciones de alta sensibilidad, tal como el grupo especial táctico de la Policía Nacional del Ecuador (GIR).

Mediante la puesta en marcha de marcos de seguridad reconocidos, se aspira a identificar y atenuar los riesgos asociados con la administración de información, la auditoría facilita la evaluación de las vulnerabilidades inherentes a los sistemas, garantizando la adhesión a las regulaciones pertinentes y el robustecimiento de estrategias apropiadas que aseguren la confidencialidad, integridad y accesibilidad de los datos esenciales para la operación policial [43].

Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador, esta investigación se enfoca en la instauración de protocolos de seguridad informática orientados a salvaguardar la información personal del Grupo de Intervención y Rescate de la Policía Nacional del Ecuador.

Mediante un análisis meticuloso, se detectan vulnerabilidades y se sugieren estrategias holísticas que se alinean con la ley orgánica de protección de datos personales, la auditoría informática facilitará la formulación de protocolos eficaces para la administración de información delicada, asegurando de este modo la integridad, confidencialidad y disponibilidad de los datos, componentes esenciales en el actual escenario de amenazas cibernéticas [44].

2.2.5 Levantamiento de información del GIR.

El Grupo de Intervención y Rescate (GIR) es una de las unidades más especializadas de la Policía Nacional del Ecuador, esta entidad compuesta por personal altamente calificado, juega un papel crucial en la seguridad nacional, dado que su intervención no solo salva vidas, sino que también consolida la confianza social en las entidades responsables de preservar el orden público. La salvaguarda de la identidad de los componentes tácticos policiales en una unidad de élite es de vital importancia por motivos de seguridad operativa y personal, la divulgación de sus identidades puede poner en peligro las misiones, amenazar sus vidas y las de sus familias o propiciar represalias por parte de agrupaciones delictivas, adicionalmente, la preservación del anonimato asegura la eficacia en operaciones encubiertas y previene intervenciones externas.

Esta salvaguarda fortalece la confidencialidad, integridad y éxito operativo, garantizando que los agentes puedan desempeñar sus funciones sin poner en riesgo su seguridad personal ni la de la institución, sin embargo, detrás de su operatividad y éxito en el campo, existe una estructura administrativa que sostiene su funcionamiento, entre la cual destaca el departamento de talento humano, encargado de gestionar la información vital de sus miembros, que por ahora protegen su identidad físicamente como se muestra en la Fig. 4.

Fig. 4. Elemento táctico del GIR

El GIR lleva a cabo una amplia gama de actividades que requieren precisión, disciplina y un alto nivel de preparación, entre sus principales funciones se encuentran las operaciones de rescate en desastres naturales, como terremotos o inundaciones, donde realizan labores de búsqueda y rescate de personas atrapadas, también intervienen en situaciones de alto riesgo, como secuestros o enfrentamientos con grupos delictivos, neutralizando amenazas y garantizando la seguridad de los afectados, protegen instalaciones estratégicas, como aeropuertos o centrales eléctricas, y participan en programas de capacitación y entrenamiento continuo para mantener su nivel de excelencia, el departamento de talento humano del GIR es responsable de gestionar la información relacionada con los miembros de esta unidad élite, esto incluye datos personales, historiales médicos, registros de capacitación y evaluaciones de desempeño.

Durante el levantamiento de información realizado en esta investigación, se identificaron varias debilidades en los sistemas informáticos y procesos utilizados por este departamento, actualmente, el departamento está conformado por personas, quienes, a pesar de su dedicación, enfrentan limitaciones significativas en términos de conocimientos técnicos y herramientas tecnológicas, entre las principales debilidades identificadas se encuentra la falta de conocimientos en ofimática por parte del personal encargado, esto dificulta la organización y análisis de la información, generando ineficiencias en los procesos administrativos, una ventaja fundamental de implementar cobit 2019 en el proceso de reclutamiento para una unidad de élite de la policía nacional radica en la normalización y optimización de la administración de riesgos y controles, esto garantiza la selección del personal más competente y fiable, maximizando la transparencia, eficiencia y seguridad del proceso, al tiempo que se alinea con los objetivos estratégicos de la institución y se adhieren a las regulaciones y estándares de calidad establecidos.

La gestión del talento humano se realiza principalmente a través de tablas de excel, una herramienta que, aunque útil, resulta insuficiente para manejar la complejidad y el volumen de datos que requiere una unidad como el GIR, este enfoque manual aumenta el riesgo de errores y limita la capacidad de generar reportes o análisis en tiempo real, en la Fig. 5 podemos ver como registran actividades en un pizarrón.

Fig. 5. Secretario del departamento de talento humano.

Otra debilidad importante es la falta de sistemas informáticos sofisticados, el departamento no cuenta con herramientas especializadas para la gestión del talento humano, lo que contrasta con las necesidades de una unidad de élite, donde la información debe ser accesible, segura y actualizada constantemente, además, la seguridad de la información no es robusta, ya que no existen protocolos claros ni herramientas tecnológicas adecuadas para proteger los datos sensibles.

Esto expone la información a riesgos como accesos no autorizados, pérdida de datos o ciber-ataques, la realización de una auditoría de sistemas informáticos en el departamento de talento humano del GIR no solo es necesaria, sino urgente, esta auditoría permitirá identificar las vul-nerabilidades existentes y proponer soluciones que fortalezcan la gestión administrativa de la unidad.

La auditoría nos permitió ver con mucha más claridad varias cosas que antes pasaban des-apercibidas, gracias a este proceso, pudimos crear protocolos de seguridad más sólidos, pensados para proteger no solo los datos personales, sino también la información estratégica del GIR, lo que ayuda bastante a reducir el riesgo de fugas, además, mientras avanzábamos en la revisión, nos dimos cuenta de que también era posible reorganizar mejor el uso del recurso humano, es-to fue factible porque ahora contamos con tecnología más actualizada, lo que, poco a poco, ha permitido que el equipo se enfoque en tareas con mayor valor y trabaje de una manera más

productiva. Al final, todo esto termina aportando directamente a la seguridad nacional, porque un GIR que funciona bien, que está preparado y que mantiene su capacidad operativa, puede proteger mejor a la ciudadanía y reaccionar de forma adecuada cuando surge una emergencia.

El GIR, constituye un componente indispensable para la seguridad de Ecuador, cuyo trabajo tiene un impacto directo en la salvaguarda de vidas y la preservación del orden público, sin embargo, su eficacia no depende únicamente de las operaciones en el campo, sino también de una gestión administrativa sólida y moderna, la evaluación de los sistemas informáticos empleados en el departamento de talento humano constituye una oportunidad inestimable para identificar áreas de mejora, robusteció la seguridad de la información y perfeccionó los procesos que sustentan la operatividad de esta unidad de alta capacidad.

Mediante la atención a estas vulnerabilidades, no solo aumenta el éxito operativo del GIR, sino también se fomenta el bienestar social de Ecuador, es por eso muy importante conocer el organigrama de la Unidad Nacional del Intervención y Rescate a nivel país como se muestra en la Fig. 6 .

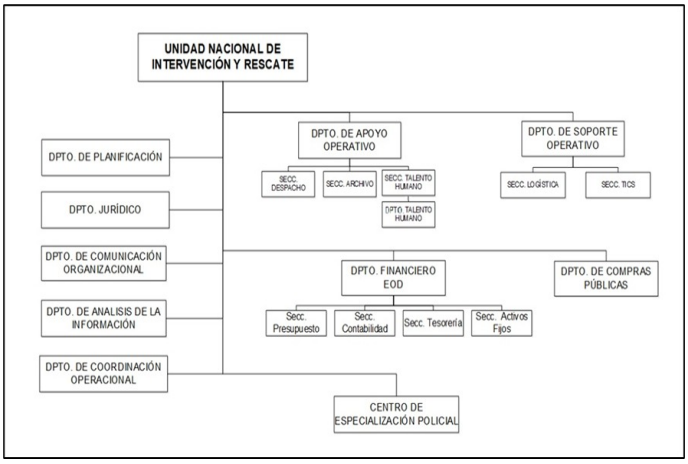

Fig. 6. Organigrama del GIR

La auditoría informática en el GIR consideró no solo las debilidades técnicas, sino también los sesgos sistémicos que pueden afectar la toma de decisiones, los sistemas automatizados, como los utilizados en la gestión del talento humano, pueden perpetuar sesgos si no se auditan adecuadamente [45], alternativamente, un enfoque de auditoría personalizado para contextos particulares, como el de las unidades de élite, es fundamental para asegurar la efectividad y la protección de los sistemas informáticos [46].

2.2.6 Sistemas informáticos utilizados actualmente en el GIR.

Infraestructura de Hardware.

El departamento de Talento Humano cuenta con 3 computadoras de escritorio para realizar sus actividades diarias, estas computadoras son utilizadas por los 3 secretarios y el jefe de departamento, los otros departamentos del GIR cuentan con equipos de computación propios.

Los equipos tienen procesadores Intel Core i5, 8 GB de RAM y almacenamiento en disco duro de 500 GB, los dispositivos presentan un rendimiento adecuado para tareas básicas, pero se observa lentitud al ejecutar aplicaciones simultáneas o de alto consumo de recursos, se cuenta con routers, switches, impresoras multifuncionales y escáneres para la gestión documental. Además, la unidad policial dispone de servidores locales para el almacenamiento centralizado de datos, como podemos ver en la Fig. 7 de tipología de red del departamento de talento humano del GIR.

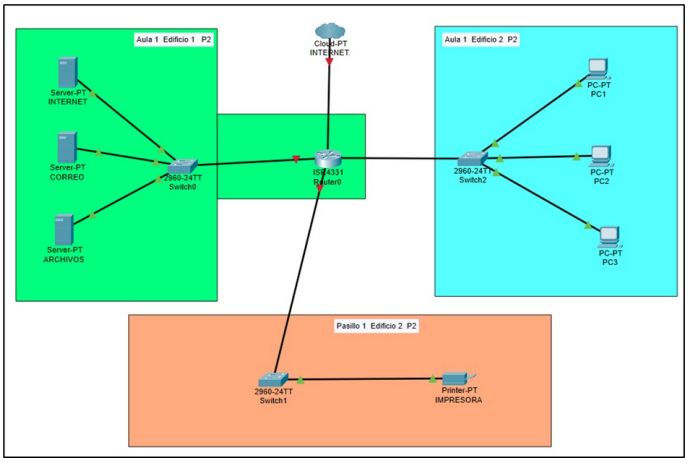

Fig. 7. Tipología física de red del departamento de talento humano del GIR

Comunicación con otras dependencias.

Sistema quipux: Es un sistema utilizado para recibir y enviar información a otras unidades policiales.

Sistema SIIPNE 3W de la policía nacional: Plataforma dedicada a la emisión y recepción de notificaciones oficiales, así como también para ver las hojas de vida de los servidores policiales.

Capacitación y evaluación.

Sistema eduvirtual: Plataforma utilizada para la capacitación del personal, permite la impartición de cursos virtuales y el seguimiento del progreso de los participantes.

Sistema de evaluación de desempeño: La herramienta nos sirve para medir el rendimiento anual del personal Como resultado tenemos los indicadores que ya revisaron.

Comunicación Interna

Plataformas de correo electrónico y mensajería instantánea: Utilizadas para la coordinación entre departamentos, servicios de Google como Gmail y de Microsoft como Outlook.

Herramientas de colaboración: Estas facilitan la comunicación y el trabajo en equipo por ejemplo Teams.

Conectividad y redes.

Red local (LAN): Las computadoras están conectadas a una red local que permite el intercambio de información entre los equipos del departamento.

Acceso a internet: La conexión de banda ancha que tenemos resulta suficiente por ello para lo básico navegar y revisar el correo del mismo modo sin mayor problema el asunto se complica cuando necesitamos plataformas en la nube o videollamadas; ahí notamos que la velocidad se queda corta y el ritmo de trabajo se baja.

Almacenamiento y seguridad de datos

Almacenamiento local: Los datos más críticos desde el historial laboral hasta las sanciones se guardan directamente en discos duros locales y archivos de Excel. Nos dimos cuenta de que esto es un verdadero riesgo; un fallo en uno de esos equipos podría suponer la pérdida total de la información, ya que no existen copias de seguridad robustas.

Falta de servidores centralizados: No hay ningún servidor, ni local ni en la nube, que unifique y gestione toda esta información cada cual termina guardando los datos en su propio ordenador.

Seguridad informática: Echamos en falta medidas de seguridad más sólidas, no encontramos firewalls, antivirus corporativos ni sistemas que alerten de accesos no autorizados, lo que deja los datos bastante expuestos.

Hallazgos y observaciones

Falta de una plataforma de desarrollo profesional: No existe una herramienta que centralice la formación y el crecimiento del equipo. Gestionar los planes de capacitación o evaluar competencias se hace de forma manual y desconectada, lo que ralentiza mucho el proceso.

Gestión descentralizada de datos: El hecho de que la información esté repartida en ordenadores locales y en hojas de Excel provoca duplicidades, inconsistencias y un peligro constante de que se pierda algo importante.

Turnos y recursos: Los secretarios rotan a diario para asegurar una vigilancia continua las 24 horas, el problema es que solo cuentan con 3 computadoras de escritorio para todo el departamento, un cuello de botella que afecta directamente a la productividad y al flujo de trabajo

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1 Tipo de investigación.

La presente investigación se clasifica como descriptiva, aplicada y documental, es de carácter descriptivo porque permite caracterizar la situación actual de los procesos de reclutamiento y gestión de información en el departamento de talento humano del Grupo de Intervención y Rescate (GIR) de la policía nacional del Ecuador, identificando las debilidades existentes en materia de seguridad informática, calidad de datos y cumplimiento normativo.

La consideramos aplicada porque va mucho más allá del simple diagnóstico, lo que hemos hecho es diseñar una hoja de ruta concreta, alineada con COBIT 2019, que busca optimizar la gobernanza de TI, blindar la información sensible y asegurar que se cumpla a rajatabla la ley de protección de datos. No nos quedamos en lo que falla, sino que trazamos el camino para solucionarlo.

Se clasifica como documental porque se fundamenta en la revisión y análisis de literatura especializada, normas técnicas, regulaciones vigentes y documentos institucionales relacionados con la seguridad de la información y el gobierno de TI, este enfoque permitió sustentar teóricamente la investigación, identificar buenas prácticas reconocidas internacionalmente y contextualizar los hallazgos obtenidos a través de encuestas, entrevistas y pruebas técnicas con herramientas como Nmap.

3.2 Metodología.

La metodología adoptada en la presente investigación responde a un enfoque mixto, combinando métodos cualitativos y cuantitativos con el propósito de analizar integralmente el proceso de reclutamiento del Grupo de Intervención y Rescate (GIR), desde la perspectiva de la gobernanza de tecnologías de la información, en conformidad con el marco de referencia Cobit 2019, el enfoque cualitativo permitió identificar y comprender las condiciones reales de gestión, control y seguridad de los sistemas, mientras que el enfoque cuantitativo facilitó la medición y análisis de los niveles de cumplimiento y percepción de los usuarios mediante datos verificables.

La metodología Delphi es una técnica de pronóstico y toma de decisiones en grupo, fundamentada en el principio de que los juicios de un grupo estructurado son más acertados que los de individuos no organizados, su objetivo principal es alcanzar un consenso entre un panel de expertos sobre un tema complejo mediante una serie de cuestionarios secuenciales y anónimos, el proceso es iterativo, en cada ronda, los expertos responden a un cuestionario, reciben un resumen anónimo de las respuestas del grupo (generalmente medidas de tendencia central) y se les solicita que reconsideren su opinión inicial a la luz de esta retroalimentación, este ciclo se repite hasta que se logra un grado estable de consenso o se agotan las rondas, el anonimato evita la influencia de personalidades dominantes y el ”pensamiento grupal”, es especialmente útil para la planificación a largo plazo, la identificación de riesgos y la priorización de temas donde no existen datos históricos suficientes, su rigurosidad sistemática lo distingue de otras técnicas de consenso cualitativas.

3.3 Población y muestra.

Para este estudio, tomamos como referencia a las 300 personas que participaron en el proceso de reclutamiento del proyecto GIR, sumamos también al equipo de tecnologías de la información, el grupo que realmente conoce y gestiona los sistemas y la seguridad de los datos en el día a día.

Para determinar el tamaño de la muestra se empleó la fórmula estadística para poblaciones finitas Ecuación 1 [47] , con un error de estimación del 6 %:

$$n = \frac{M}{e^2(M-1)+1} \tag{1}$$

donde M corresponde al tamaño de la población y e al error de estimación permitido.

Sustituyendo los valores $M = 300$ y $e = 0{,}06$ se obtiene:

$$n = \frac{300}{(0{,}06)^2(300-1)+1} \approx 145$$

Por lo tanto, el tamaño mínimo de muestra requerido fue de 145 participantes, sin embargo, en la Tabla II, en el desarrollo de este estudio se obtuvo un total de 159 respuestas válidas mediante la aplicación del formulario a los postulantes, lo que supera el número requerido y corresponde aproximadamente al 53 % de la población total, además se realizaron 2 entrevistas

al personal del área de TI, lo que permitió complementar la información con la visión técnica y de gestión.

Tabla II.
RESUMEN DE POBLACIÓN Y MUESTRA

Concepto	Valor
Población total (postulantes)	300
Muestra mínima requerida	145
Muestra obtenida (respuestas de formulario)	159
Entrevistas a personal de TI	2

Para la aplicación de la técnica de encuesta se realizo una selección aleatoria de 159 del total de los postulantes como recomienda la Ecuación 1, ya que todos los elementos de la población tenían la misma probabilidad de ser seleccionados y participar en el formulario, este tipo de muestreo resulta adecuado en grupos homogéneos donde se busca representatividad estadística.

Para el personal del área de TI se empleó un muestreo intencional o por conveniencia, al tratarse de actores clave con conocimientos técnicos específicos sobre la seguridad y la gestión de los recursos informáticos, de esta forma, la muestra efectiva integró tanto la visión de los usuarios finales (159 postulantes) como la de los responsables tecnológicos (2 funcionarios de TI) lo que permitió un análisis integral y robusto en el marco de COBIT 2019.

3.4 Técnicas e instrumentos aplicados.

3.4.1 Recopilar documentación.

Esta técnica se empleó para revisar y examinar los documentos institucionales vinculados con la gestión del talento humano y la administración tecnológica dentro del GIR, se analizaron políticas institucionales, manuales de procesos, organigramas funcionales y oficios emitidos por la dirección nacional de talento humano (DNATH), correspondientes a procesos de reclutamiento anteriores.

El objetivo fue identificar la existencia o ausencia de normativas, directrices y lineamientos que garanticen la correcta gestión de la información, el control de accesos y la seguridad tecnológica, permitiendo establecer la base conceptual y normativa sobre la que se evaluó el cumplimiento de los objetivos de control de COBIT 2019, mismo que fue verificado en el Anexo I.

3.4.2 Sistemas actuales.

Se identificaron y documentaron los sistemas informáticos utilizados en el proceso de reclutamiento y administración de personal, detallando sus funciones, responsables y mecanismos de soporte, entre ellos se encuentran el sistema integrado de información policial (SIIPNE 3W) y los registros internos administrados por la DNATH.

3.4.3 Encuestas.

Las encuestas se utilizaron para complementar la observación directa y la revisión documental, se aplicaron encuestas como técnica de recolección de información, estas se dirigieron a los usuarios internos de los sistemas informáticos del departamento de talento humano del GIR, con el objetivo de conocer su experiencia respecto al uso de los sistemas, control de accesos, respaldo de información, seguridad de los servicios y gestión de incidentes.

Las encuestas fueron elaboradas tomando como referencia la escala de madurez de Cobit 2019, lo que permitió identificar brechas significativas entre la situación actual y las buenas prácticas internacionales utilizando varios dominios, para el proceso de reclutamiento en el GIR, esta considera cinco dominios (EDM, APO, BAI, DSS, MEA) y mínimo tres subdominios por cada uno, los cuales permiten valorar diversos aspectos, desde las políticas y la supervisión de la dirección hasta la seguridad, el soporte y la auditoría de los sistemas de información involucrados, las preguntas consideradas en la encuesta se detallan en el Anexo II.

Cada ítem de encuesta se calificó con la escala del nivel de capacidad Cobit 2019 (0–5) para estimar nivel actual y brecha frente al nivel objetivo como muestra la tabla III .

Tabla III.
ESCALA DE CAPACIDAD / MADUREZ (COBIT 2019)

Nivel	Descripción
0	Incompleto
1	Realizado (Performed Process)
2	Gestionado (Managed Process)
3	Establecido (Established Process)
4	Predecible (Predictable Process)
5	Optimizado (Optimizing Process)

- **EDM01 — Mantener el marco de gobierno:** Revisamos que el proceso de reclutamiento cuente con políticas claras y documentadas, donde se definan los roles, las responsabilidades y los lineamientos estratégicos, siempre en línea con lo que exige la normativa policial y estatal.

- **EDM03 — Cumplir con lo que estipula las legislaciones:**

  Asegurándonos que se cumplan las regulaciones tales como la ley de protección de datos personales, para garantizar que la información de los candidatos y la del personal sean tratados conforme a la ley.

- **EDM04 — Optimizar la gestión de riesgos:** Se comprobó el cumplimiento de la normativa, a la vez rendición de cuentas y la protección, especialmente de aquellos datos sensibles, así como a la formalización de actuaciones e información a la dirección sobre cada una de las decisiones adoptadas.

- **APO01 — Gestionar la estrategia de TI:** Mediante esta investigación se analizó cómo la estrategia tecnológica puede alinearse con los objetivos del GIR y reforzar sus procesos internos, de este modo, se puede evidenciar que la tecnología es un apoyo de manera efectiva tanto en los ámbitos de seguridad como en la gestión del personal, este análisis permitió identificar oportunidades de mejora contribuyendo a la integración más coherente entre las metas institucionales y las capacidades tecnológicas actuales.

- **APO10 — Gestionar a los proveedores:** Evaluamos los riesgos que pueden venir de plataformas externas, tales como sistemas de mensajería o servicios en la nube,por ello revisando contratos, niveles de servicio y posibles puntos débiles en la cadena.

- **APO12 — Gestionar los riesgos:** Se identifico y analizó algunas amenazas que pueden afectar la confidencialidad, integridad o disponibilidad de la información, asimismo, consideramos los escenarios como accesos no autorizados o fallos en los sistemas actuales, lo comprendiendo de mejor manera los puntos críticos y seguido de esto, proponer medidas de mitigación más efectivas.

- **BAI03 — Gestionar las soluciones tecnológicas:** Verificamos que los sistemas utilizados en talento humano no solo cumplan con los requisitos de seguridad, sino que además garanticen la disponibilidad, estabilidad y usabilidad que una unidad de élite requiere

para operar adecuadamente, de esta manera, aseguramos que las soluciones tecnológicas respondan coherentemente a las necesidades institucionales.

- **BAI06 — Gestionar los cambios:** Se desarrolló la gestión y análisis en plataformas o procesos ya que en este sentido se necesitaba saber si existe la debida documentación, así como pruebas previas y autorizaciones formales antes de ser utilizadas, permitiéndonos la reducción de errores, el aseguramiento de la continuidad operativa y reforzar la trazabilidad de cada cambio implementado.

- **BAI07 — Asegurar la transición de los cambios:** Revisamos que cada cambio venga acompañado de la formación necesaria al personal, y de la misma manera que se validen los resultados y que se afecte lo mínimo posible la operación diaria.

- **DSS02 — Gestionar incidentes y peticiones:** Se realizó la evaluación y registgro de como actuan ante incidentes en los sistemas midiendo la eficiencia en la atención, así como el impacto que estas puedan tener en la seguridad institucional, de esta manera, se obtuvo una visión más clara de la capacidad de respuesta ante incidentes críticos.

- **DSS04 — Gestionar la continuidad:** Verificamos que existan planes de contingencia actualizados que protejan la información del personal ante fallos técnicos, desastres naturales o ciberataques, asimismo, revisamos que dichos planes consideren procedimientos de recuperación y mecanismos de respaldo que garanticen la continuidad operativa del GIR.

- **DSS05 — Gestionar la seguridad de los servicios:** Confirmamos que se hayan implementado diversas medidas de protección en los servicios de TI, tales como antivirus, firewalls y copias de seguridad, además, evaluamos que la seguridad informática respalde adecuadamente la operación del GIR y contribuya a reducir vulnerabilidades.

- **MEA01 — Supervisar el desempeño y la conformidad:** Realizamos el seguimiento a indicadores clave del área de talento humano, como los tiempos de respuesta en los procesos de reclutamiento, la calidad de los datos gestionados y el cumplimiento de las políticas institucionales, de este modo, se puede determinar si las acciones implementadas están alineadas con los objetivos del GIR.

- **MEA02 — Evaluar el control interno:** Analizamos las auditorías internas realizadas al GIR, tales como revisar si los controles aplicados en los procesos de personal y datos son realmente efectivos frente a riesgos internos y externos.
- **MEA03 — Verificar el cumplimiento externo:** Comprobamos que se atiendan de manera oportuna las observaciones realizadas por auditorías externas y, además, evaluamos cómo dichas recomendaciones se integran en los procesos internos, de esta manera, se puede garantizar una mayor transparencia y una rendición de cuentas responsable en el manejo de información crítica, asegurando que las prácticas del GIR se mantengan alineadas con los estándares establecidos.

Aplicación de la encuesta

La encuesta fue puesta en manos de los usuarios y de los responsables clave del área, por este motivo en la investigación que se presenta a continuación, se proponen algunas evidencias que permiten medir, con cifras concretas, la efectividad real de la gestión de TI en torno a cuatro ejes como son el reclutamiento y la seguridad de datos – como previene frente a un acceso no autorizado a los datos – la continuidad de la operación institucional o de servicios y la supervisión institucional.

Procedimiento

Para evaluar las respuestas de la encuesta utilizamos la escala de madurez de COBIT 2019 esta va del 0 al 5, donde 0 significa que el proceso prácticamente no existe y 5 representa un proceso que no solo funciona, sino que está perfeccionado.

a) **Codificación de respuestas:**

   Convertimos cada pregunta del cuestionario en una puntuación del 0 al 5, según la respuesta que marcó cada persona. Así pasamos de las opiniones a números concretos que pudimos analizar.

b) **Cálculo de promedios por ítem:**

   Se calculó la media aritmética de las respuestas de todos los participantes en cada ítem, esto permitió obtener un valor que representa el nivel de madurez percibido para cada pregunta.

c) **Agrupación por dominios:**

- EDM (Evaluar, Dirigir y Monitorear) (Preguntas 1 a 3)
- APO (Alinear, Planear y Organizar) (Preguntas 4 a 6)
- BAI (Construir, Adquirir e Implementar) (Preguntas 7 a 9)
- DSS (Entregar, Dar Servicio y Soportar) (Preguntas 10 a 12)
- MEA (Monitorear, Evaluar y Valorar) (Preguntas 13 a 15)

Para el análisis de los resultados de la encuesta se aplicaron medidas estadísticas descriptivas, entre ellas la media aritmética y la desviación estándar .

Media aritmética. Ecuación 2[48]:

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \tag{2}$$

donde $\bar{x}$ representa la media, x_i los valores observados y n el número total de observaciones.

Desviación estándar. Ecuación 3[49]:

$$s = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})^2} \tag{3}$$

La ecuación 3 corresponde a la desviación estándar muestral, donde s representa la desviación, x_i son los valores de cada observación, $\bar{x}$ la media aritmética y n el tamaño de la muestra.

3.4.4 Entrevistas.

La entrevista se utilizó para recopilar información cualitativa y cuantitativa que permitiera identificar el nivel de madurez y efectividad de los controles de TI establecidos en el marco Cobit 2019, a través de un cuestionario estructurado aplicado al personal del departamento de TI, se evaluó la existencia, aplicación y documentación de los controles, las respuestas obtenidas, clasificadas en una matriz, sirvieron como base para diagnosticar fortalezas, debilidades y oportunidades de mejora, fundamentando así la posterior formulación de un plan de acción para el fortalecimiento de la gobernanza de TI en la institución.

El cuestionario de entrevista presenta el detalle del temario aplicado al departamento de TI, organizado por dominios y subdominios de Cobit 2019, este formato permitió garantizar que cada pregunta estuviera vinculada directamente con los controles específicos a evaluar, facilitando

la posterior clasificación de respuestas en la matriz de madurez, este instrumento considera cinco dominios (EDM, APO, BAI, DSS, MEA) y tres subdominios por cada uno como se detallan en el Anexo III.

Detalle del proceso de entrevista.

a) **Objetivo de la entrevista.**

El objetivo principal de la entrevista aplicada al área de tecnologías de la información (TI) fue recopilar información cualitativa y cuantitativa que permitiera identificar el nivel de madurez y efectividad de los controles establecidos en el marco Cobit 2019, este levantamiento de información constituye la base para la construcción de la matriz de evaluación de controles, con el fin de determinar fortalezas, debilidades y oportunidades de mejora en la gestión de la gobernanza de TI.

b) **Participantes.**

La entrevista fue dirigida al personal del departamento de tecnologías de la información, quienes poseen conocimiento directo sobre la infraestructura tecnológica, la gestión de riesgos, la seguridad informática y el soporte a procesos estratégicos de la institución, el proceso fue conducido por el investigador, quien actuó como moderador, registrador y evaluador de las respuestas obtenidas.

c) **Diseño metodológico.**

La entrevista se desarrolló a partir de un cuestionario estructurado basado en los procesos y dominios del marco Cobit 2019 (EDM, APO, BAI, DSS y MEA), el cuestionario se elaboró con el propósito de verificar la existencia, aplicación y documentación de controles de TI, considerando tres criterios de evaluación:

- ✓ **Sí:** El control se encuentra implementado y documentado formalmente.
- ✗ **No:** El control no está implementado
- ∂ **Parcialmente:** Este control está de manera incompleta.

d) **Procedimiento de aplicación**

La entrevista se aplicó de manera presencial, en un espacio de diálogo abierto que permitió a los entrevistados detallar el estado actual de las prácticas de TI, las respuestas fueron registradas en un formato digital (Excel), lo cual facilitó la sistematización y posterior cruce de datos con la matriz de evaluación, posteriormente, la información fue contrastada

con los controles definidos en cobit 2019 para establecer un diagnóstico preliminar de madurez institucional.

e) **Instrumento aplicado.**

El cuestionario incluyo preguntas que se relacionan con los diversos aspectos claves que tiene el marco COBIT 2019, permitiendo obtener una mejor visión integral del funcionamiento actual de los procesos evaluados profundizando en los siguientes componentes:

- **EDM:** Para identificar el grado de alineación con los objetivos organizacionales se tomo en cuenta políticas institucionales, cumplimiento normativo y gestión de riesgos estratégicos.
- **APO:** Se realizó la evaluación y registro de como actúan ante incidentes en los sistemas midiendo la eficiencia en la atención, así como el impacto que estas puedan tener en la seguridad institucional, de esta manera, se obtuvo una visión más clara de la capacidad de respuesta ante incidentes críticos.
- **BAI:** Se evaluaron las soluciones tecnológicas para mantener estabilidad y confiabilidad, mediante la selección de software, evaluación de seguridad en los cambios y pruebas de aceptación antes de la puesta en producción, asegurando que las soluciones tecnológicas se mantengan.
- **DSS:** El análisis del dominio permitió diseccionar la arquitectura de resiliencia operativa, identificando las salvaguardas de autenticación y los protocolos de mitigación de brechas ante eventos disruptivos en la gestión de incidentes.
- **MEA:** Se establece metricas para determinar los indicadores y evaluación de la efectividad en las medidas implementadas, lo que permitió valorar si los procesos cumplen los resultados esperados.

f) **Respuestas Obtenidas.**

Analizamos las respuestas en la matriz de evaluación y el panorama quedó bastante claro, por un lado encontramos fortalezas sólidas en la planificación estratégica, la gestión de riesgos, el trato con proveedores, los cambios de software y cómo manejan los incidentes, también detectamos puntos flacos importantes especialmente en el cumplimiento normativo, la continuidad del servicio, la seguridad de la información y los procesos de auditoría.

Un caso particular fue la evaluación de medidas para mitigar riesgos, donde los resultados fueron dispares, este diagnóstico con sus luces y sombras es el cimiento sobre el que construimos el plan de acción, un proyecto pensado para fortalecer de manera integral toda la gobernanza y gestión de TI de la institución.

En el marco de la presente investigación, se diseñó un cuestionario estructurado con base en los dominios y procesos definidos por el marco Cobit 2019, dicho instrumento permitió recopilar información sobre las prácticas actuales del área de tecnologías de la información en relación con la gestión de riesgos, cumplimiento normativo, continuidad del servicio y procesos de soporte.

3.4.5 Checklist.

La entrevista aplicada al departamento de tecnologías de la información fue complementada con la utilización del checklist basado en Cobit 2019, este instrumento permitió contrastar las respuestas obtenidas con los controles y prácticas establecidas en dicho marco, facilitando la identificación del nivel de cumplimiento de cada dominio y subdominio evaluado se detallan en el Anexo IV, de esta manera, se garantizó que la información levantada no solo se limite a percepciones del personal entrevistado, sino que sea validada mediante un estándar internacionalmente reconocido, aportando mayor rigor al diagnóstico de madurez

Conocida como técnica de lista de verificación, se utilizó un instrumento basado en los dominios y objetivos de control de CObit 2019, enfocado en la revisión del cumplimiento de los procesos de gobernanza y gestión de TI, especialmente en las áreas de seguridad, disponibilidad, continuidad de servicios y control de incidentes, facilitando la evaluación estructurada de las condiciones del entorno tecnológico, identificando brechas específicas en la implementación de buenas prácticas.

La entrevista se desarrolló a partir de un cuestionario estructurado basado en los procesos y dominios del marco Cobit 2019 (EDM, APO, BAI, DSS y MEA), el cuestionario se elaboró con el propósito de verificar la existencia, aplicación y documentación de controles de TI, considerando tres criterios de evaluación:

- ✓ Sí: El control se encuentra implementado y documentado formalmente.
- ✗ No: Este control no está implementado.
- ∂ Parcialmente: Este control está presente pero de manera incompleta.

3.4.6 Pruebas técnicas – escaneo Nmap.

Con el propósito de identificar vulnerabilidades en la infraestructura tecnológica utilizada en el proceso de reclutamiento del Grupo de Intervención y Rescate, se realizó un conjunto de escaneos técnicos mediante la herramienta Nmap, este análisis tuvo como finalidad evaluar los sistemas operativos, las configuraciones de red, los servicios activos y las aplicaciones involucradas en la gestión de datos personales y administrativos del personal aspirante.

El procedimiento permitió examinar los equipos pertenecientes a tres dependencias críticas, el departamento de talento humano, la oficina de secretaría y la oficina de tecnologías de la información como se puede observar en el Anexo V, la información obtenida fue analizada para determinar los servicios expuestos, la existencia de puertos abiertos y las posibles vulnerabilidades que podrían comprometer la seguridad, confidencialidad e integridad de la información procesada durante las etapas de reclutamiento.

La aplicación combinada de estas técnicas permitió obtener una comprensión completa de la situación actual del proceso de reclutamiento, ya que, al contrastar la percepción de los usuarios con la evidencia documental y técnica, se garantizó la validez de los resultados, asimismo, esta triangulación de información facilitó identificar coincidencias y brechas relevantes, de este modo, fue posible establecer un diagnóstico sólido y bien fundamentado, sobre el cual se construyó la propuesta de mejora alineada al marco COBIT 2019, garantizando coherencia entre los hallazgos y las acciones sugeridas.

3.5 Diagrama de procedimiento de auditoría.

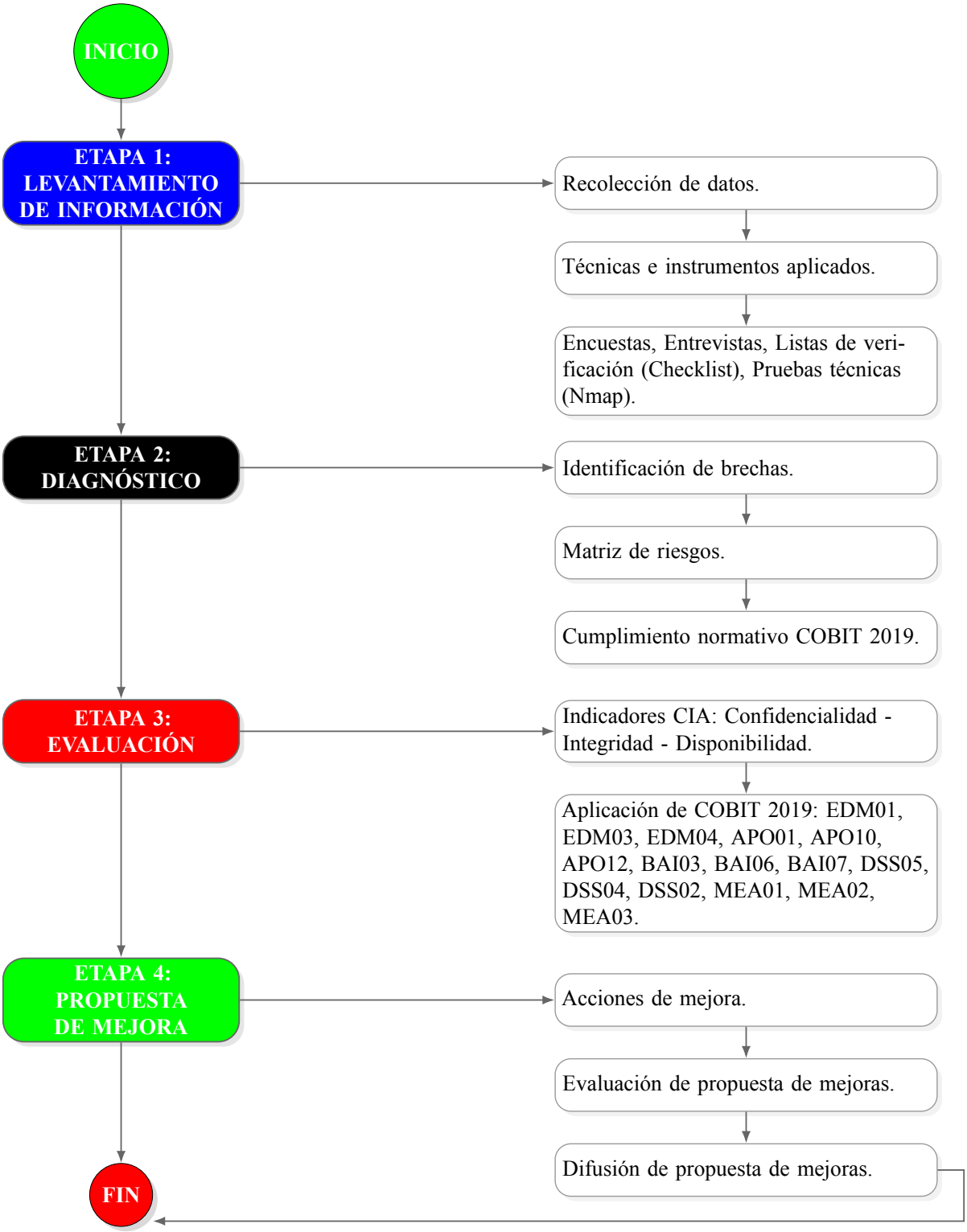

Fig. 8. Metodología de auditoría de TI basada en COBIT 2019.

Bajo el esquema metodológico ilustrado en la Figura 8, se ejecutó una fiscalización sistémica articulada en cuatro estadios operativos, cuya descripción técnica se detalla a continuación.

Etapa 1: Levantamiento de Información. Esta fase inicial se orientó a la obtención de una visión holística del ecosistema tecnológico y sus flujos de trabajo mediante técnicas de recolección multidimensional:

- **Análisis documental:** Se auditaron registros históricos y protocolos de las promociones XXI y XXII, suministrados por la DNATH, con el fin de mapear la trazabilidad de los datos y la vigencia de los marcos procedimentales.
- **Aplicación de encuestas::** Se desplegó un cuestionario a 159 aspirantes, parametrizado bajo los niveles de madurez de COBIT 2019 (escala 0-5), para cuantificar la observancia percibida en torno a la tríada CIA y la gestión del ciclo de vida del reclutamiento.
- **Entrevistas al personal de TI:** Se mantuvieron sesiones semiestructuradas con los responsables de infraestructura para contrastar la operatividad real frente a la documentación oficial de los dominios COBIT 2019.
- **Validación mediante Checklists:** Se emplearon listas de cotejo estandarizadas para realizar un *cross-check* entre las aserciones del personal y el cumplimiento normativo del marco de gobernanza.
- **Pruebas técnicas con Nmap:** Se efectuó un reconocimiento de activos y servicios en las capas de transporte y aplicación de las áreas de Talento Humano, Secretaría y TI, identificando vectores de riesgo, puertos expuestos y vulnerabilidades críticas.

Esta fase consolidó un repositorio de evidencia técnica sustancial para fundamentar el diagnóstico de madurez y la remediación posterior.

Etapa 2: Diagnóstico. Tras la fase de reconocimiento, se procedió a la síntesis analítica de los hallazgos para determinar la postura de seguridad actual:

- **Identificación de brechas:** Se contrastó el nivel de madurez empírico (promedio de 3.33) frente al umbral de optimización definido (Nivel 4 - Predecible), desagregando la desviación en los dominios EDM, APO, BAI, DSS y MEA.
- **Elaboración de la Matriz de Riesgos:** Se categorizaron amenazas de exfiltración y denegación de servicio según su probabilidad e impacto sistémico, priorizando aquellos activos de información con mayor exposición.

- **Análisis de cumplimiento normativo:** Se midió la alineación con los subdominios de COBIT 2019, detectando fortalezas relativas en APO12 y deficiencias críticas en la seguridad de servicios (DSS05) y supervisión interna (MEA02).

Etapa 3: Evaluación. En esta instancia, el análisis se profundizó mediante criterios transversales de seguridad informática:

- **Auditoría bajo el modelo CIA:** Se examinó el rendimiento operativo basándose en tres pilares:
    - **Confidencialidad:** Fiscalizando la granularidad de los controles de acceso a datos sensibles.
    - **Integridad:** Verificando la inalterabilidad de los registros históricos de los candidatos.
    - **Disponibilidad:** Analizando la redundancia de sistemas y la capacidad de recuperación ante desastres.
- **Evaluación detallada con COBIT 2019:** Se ejecutó una inspección exhaustiva de 5 dominios y 16 subdominios específicos, determinando el grado de cumplimiento de las prácticas de gestión para asegurar un gobierno de TI resiliente.

Etapa 4: Propuesta de Mejora y Validación. La fase concluyente consistió en el diseño de salvaguardas y su legitimación por pares expertos:

- **Formulación de acciones de mejora:** Se formularon 36 controles técnicos y administrativos, alineados con COBIT 2019, para neutralizar los vectores de ataque identificados en el reclutamiento.
- **Evaluación de la propuesta mediante el método Delphi:** Un panel de 7 especialistas evaluó la propuesta en dos ciclos. La dispersión inicial ($W = 0{,}361$) fue corregida mediante retroalimentación estructurada, alcanzando una convergencia absoluta ($W = 1{,}00$) en la segunda ronda.
- **Difusión de la propuesta:** Se formalizó un Plan de Seguridad robusto, orientado a su socialización en el GIR para garantizar la protección de datos y la optimización de la gobernanza institucional.

CAPÍTULO IV
RESULTADOS Y ANÁLISIS

4.1 Etapa 1: Levantamiento de información.

4.1.1 Resultados del análisis documental.

El diagnóstico evidenció la inexistencia de políticas claras y documentadas, así como debilidades en la gestión de riesgos, continuidad y seguridad de los servicios tecnológicos, para el análisis se consideraron los siguientes dominios y subdominios del marco de referencia Cobit 2019:

- Optimización del riesgo (EDM04)
- Gestión de proveedores (APO10)
- Gestión de riesgos de TI (APO12)
- Gestión de soluciones e implementación de cambios (BAI03, BAI06, BAI07)
- Gestión de incidentes, continuidad y seguridad de los servicios (DSS02, DSS04, DSS05)
- Monitoreo, evaluación y control interno (MEA01, MEA02, MEA03)

Entre las actividades desarrolladas se incluyeron:

a) **Evaluación de documentación y políticas existentes**

- **Estado actual:** El Grupo de Intervención y Rescate (GIR) no cuenta con documentación formalizada ni políticas específicas que regulen el uso, gestión y mantenimiento de los sistemas informáticos aplicados al talento humano, tampoco existen lineamientos claros sobre control de accesos, respaldo de información o manejo de proveedores tecnológicos.
- **Implicaciones:** La falta de estas directrices crea un entorno vulnerable, en el cual no es posible garantizar que los datos del personal policial se mantengan realmente

seguros, disponibles o con su integridad preservada, como consecuencia, esta situación no solo limita la capacidad de realizar auditorías internas con el rigor necesario, sino que además complica la planificación de mejoras tecnológicas, aún más, lo que resulta especialmente preocupante, es que deja al área expuesta a posibles incumplimientos normativos y a riesgos de ciberseguridad que, con una adecuada gestión, podrían prevenirse de manera efectiva.

b) **Revisión de registros históricos de reclutamientos anteriores.**

- Se analizaron los oficios e informes emitidos por la dirección nacional de administración de talento humano (DNATH) de la policía nacional del Ecuador, entre ellos los documentos:
  - Oficio Nro. PN-DNTH-DEIN-2022-0605 de 22 de abril de 2022 y el informe ejecutivo Nro. PN-DNTH-DEIN-2022-0139, relacionados con el proceso de postulación de la XXI promoción del curso avanzado del Grupo de Intervención y Rescate (GIR).
  - Oficio Nro. PN-DNTH-DEIN-2024-00473 de 21 de febrero de 2024, que autoriza el inicio del proceso de postulación correspondiente a la XXII promoción del curso avanzado del GIR, incluyendo el informe Nro. PN-DNTH-DEIN-2024-0159-INF sobre las vacantes al orgánico de 2024.
- Los registros de la XXI promoción muestran que en el año 2022 se inscribieron 405 aspirantes en el sistema SIIPNE 3W, de los cuales 282 cumplieron los requisitos y 140 fueron declarados aptos tras la validación final, mientras que 265 fueron considerados no aptos por incumplimientos administrativos o disciplinarios, en tanto, el análisis del proceso 2024 evidenció un déficit de 105 servidores policiales, lo que motivó la apertura de nuevas vacantes en los grados de Cabo Segundo y Policía para cubrir el relevo generacional del personal operativo.
- Esta revisión nos dío una mejor visión y permitió identificar los flujos de información, los formatos empleados y las falencias en el almacenamiento y la seguridad de los datos históricos, respaldando la necesidad de implementar un sistema informático centralizado que asegure la trazabilidad, integridad y disponibilidad de la información, que genere seguridad durante los procesos de reclutamiento, asimismo, el análisis diagnostico la falta de un repositorio único que dificulta el control, la

consulta y la conservación adecuada de los registros, por lo que contar con una plataforma integrada se vuelve fundamental para mejorar la eficiencia y reducir riesgos operativos.

La documentación que incorporamos nos permitió confirmar cómo funciona realmente el departamento de talento humano del GIR, con esos papeles sobre la mesa, el diagnóstico dejó de ser una suposición para convertirse en algo tangible, dándole un respaldo sólido a todas las conclusiones que presentamos en este estudio.

4.1.2 Resultado de encuesta aplicada.

La encuesta fue contestada de la siguiente manera:

En la Fig. 9 se muestra la respuesta a la pregunta 1: ¿Existen políticas claras que regulan el uso de TI en el proceso de reclutamiento?

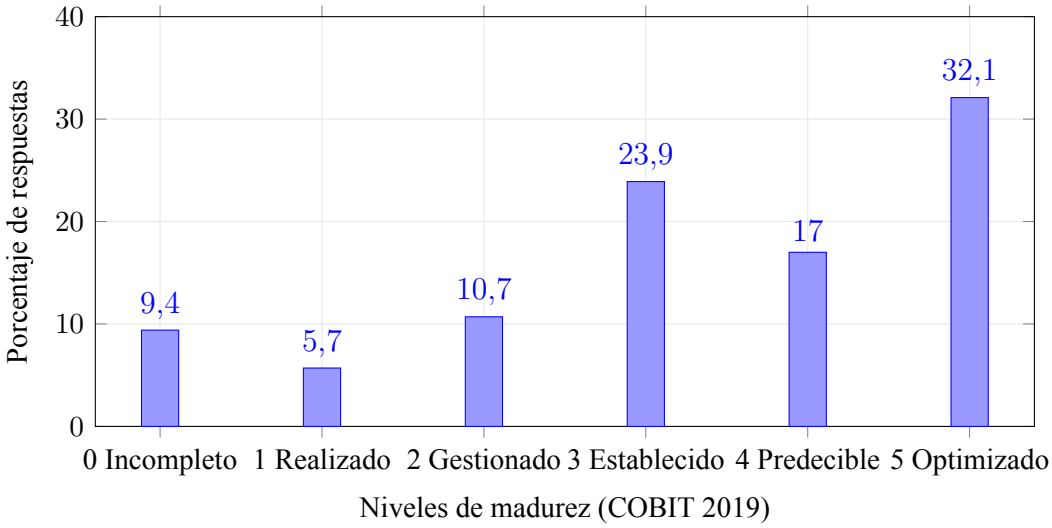

Fig. 9. Google Forms: ¿Existen políticas claras que regulan el uso de TI en el proceso de reclutamiento?

Distribución de respuestas:

- 9.4 % en el nivel 0 – Incompleto.
- 5.7 % en el nivel 1 – Realizado.
- 10.7 % en el nivel 2 – Gestionado.
- 23.9 % en el nivel 3 – Establecido.
- 17 % en el nivel 4 – Predecible.

- 32.1 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (49.1 %):** Los niveles muestran que muchos encuestados estuvieron de acuerdo en que hay políticas formales y actualizadas que se aplican de manera coherente en el proceso de reclutamiento. Asimismo, en el nivel 5 se observa que estas políticas se revisan y actualizan periódicamente, manteniéndose así alineadas con los objetivos institucionales.

b) **Niveles 2 y 3 (34.6 %):** Como se puede observar la institución cuenta con políticas definidas; sin embargo, aún se encuentran en una fase incipiente, ya que no están completamente integradas ni actualizadas, y en muchos casos la aplicación depende de iniciativas aisladas o de la voluntad individual de algunos colaboradores

c) **Niveles 0 y 1 (15.1 %):** Aquí el panorama es más crítico, pues encontramos áreas que no cuentan con documentación formal o, en su defecto, en las que las políticas de TI se aplican de manera completamente improvisada. Como resultado, esta situación genera riesgos importantes en el gobierno de la información, en el control de accesos y, especialmente, en la protección de datos sensibles. Asimismo, se evidencia una ausencia de lineamientos básicos que permitan estandarizar los procesos, lo que incrementa la vulnerabilidad institucional y dificulta cualquier intento de mejora estructurada.

En la Fig. 10 se muestra la respuesta a la pregunta 2: ¿La dirección supervisa el cumplimiento de normativas sobre seguridad de datos personales?

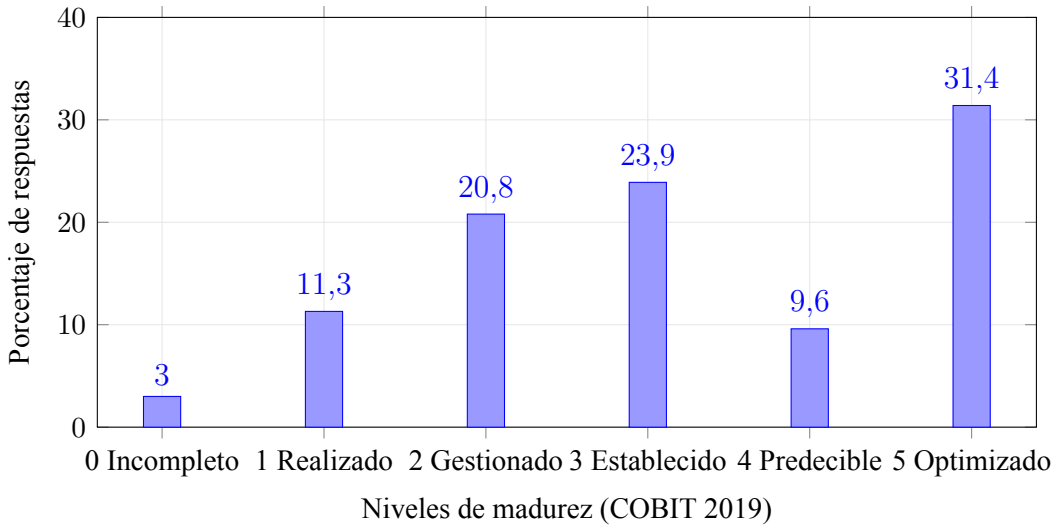

Fig. 10. Google Forms: ¿La dirección supervisa el cumplimiento de normativas sobre seguridad de datos personales?

Distribución de respuestas:

- 3 % en el nivel 0 – Incompleto.
- 11.3 % en el nivel 1 – Realizado.
- 20.8 % en el nivel 2 – Gestionado.
- 23.9 % en el nivel 3 – Establecido.
- 9.6 % en el nivel 4 – Predecible.
- 31.4 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (41 %):** Evidencian que una parte importante de los encuestados percibe un control formal y sostenido sobre el cumplimiento de las normativas de seguridad de datos personales. En este sentido, los resultados sugieren la existencia de procesos definidos, monitoreados y alineados con las exigencias legales, tales como la Ley Orgánica de Protección de Datos Personales (LOPDP). Asimismo, esta percepción refleja un nivel de madurez en el que las prácticas de seguridad no solo están documentadas, sino que también se aplican de manera consistente y responden a estándares regulatorios vigentes.

b) **Niveles 2 y 3 (44.7 %):** Según estos niveles se evidenció que la institución cuenta con procesos establecidos, aunque aún en desarrollo, existiendo una intención clara de cumplimiento normativo, la gestión requiere actualización continua para alinearse debidamente con las exigencias legales.

c) **Niveles 0 y 1 (14.3 %):** En este caso el cumplimiento normativo es frágil ya que se espera que aparezca un fallo para intervenir, porque actúa únicamente cuando surgen problemas, no existen estrategias preventivas ni controles estandarizados que garanticen la protección sistemática de la información, incrementando significativamente el riesgo institucional.

En la Fig. 11 se muestra la respuesta a la pregunta 3: *¿Los riesgos relacionados con TI en reclutamiento son identificados y monitoreados?*

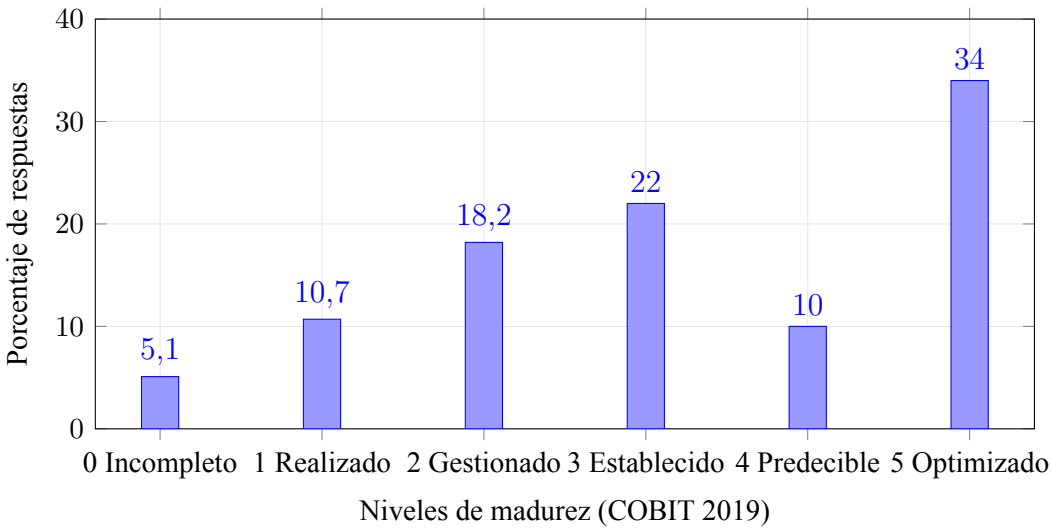

Fig. 11. Google Forms: ¿Los riesgos relacionados con TI en reclutamiento son identificados y monitoreados?

Distribución de respuestas:

- 5.1 % en el nivel 0 – Incompleto.
- 10.7 % en el nivel 1 – Realizado.
- 18.2 % en el nivel 2 – Gestionado.
- 22 % en el nivel 3 – Establecido.
- 10 % en el nivel 4 – Predecible.
- 34 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (44 %):** El nivel de madurez en el que se encuentra la institución permite gestionar los riesgos de manera proactiva, que cuenta con procesos sólidos para identificar, evaluar y monitorear los riesgos tecnológicos ya que mantiene registros actualizados y se han implementado controles que operan de manera estable que reducen la probabilidad de incidentes que afecten la continuidad operativa.

b) **Niveles 2 y 3 (40.2 %):** Se identificó que tienen controles básicos establecidos, sin embargo, la gestión de riesgos está en desarrollo, no mantienen seguimiento sistemático,además la evaluación de amenazas depende de esfuerzos aislados dentro del equipo técnico, evidenciando una carencia de documentación formal que respalde el proceso.

c) **Niveles 0 y 1 (15.8 %):** Estos niveles revelan que existe un importante vacío en la detección oportuna de riesgos ya que tiene una aproximación que es reactiva, no existen metodologías definidas ni herramientas estandarizadas, dicha situación incrementa significativamente la vulnerabilidad institucional ante incidentes de seguridad y fallos tecnológicos.

En la Fig. 12 se muestra la respuesta a la pregunta 4: ¿Los recursos de TI asignados al proceso de reclutamiento son suficientes y adecuados?

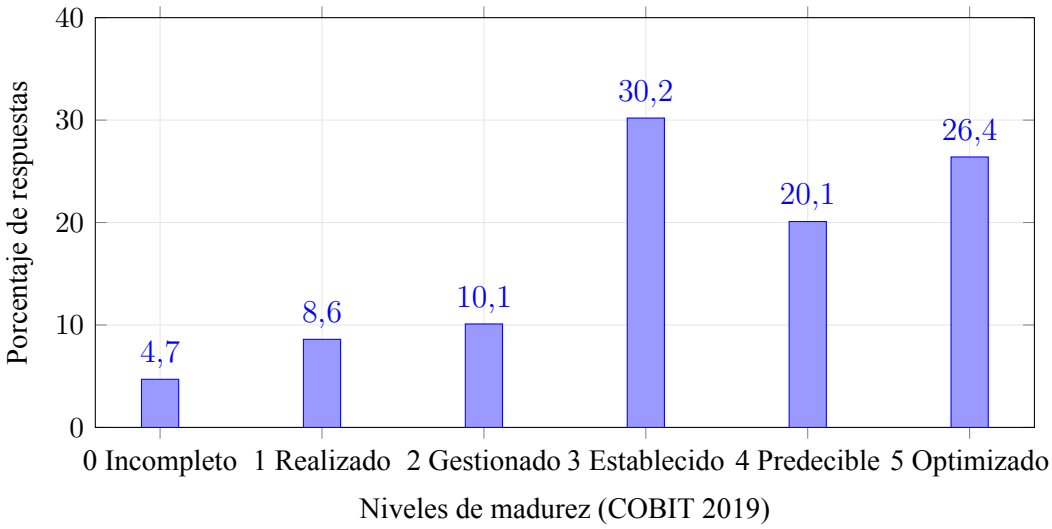

Fig. 12. Google Forms: ¿Los recursos de TI asignados al proceso de reclutamiento son suficientes y adecuados?

Distribución de respuestas:

- 4.7 % en el nivel 0 – Incompleto.
- 8.6 % en el nivel 1 – Realizado.
- 10.1 % en el nivel 2 – Gestionado.
- 30.2 % en el nivel 3 – Establecido.
- 20.1 % en el nivel 4 – Predecible.
- 26.4 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (46.5 %):** La institución sí cuenta con recursos tecnológicos que responden de manera adecuada a las necesidades del reclutamiento, también existe una planificación clara para la dotación de equipos y software, que es respaldada por soporte técnico oportuno y prácticas orientadas a la mejora continua.

b) **Niveles 2 y 3 (40.3 %):** La gestión de recursos evidencia un desarrollo intermedio, si bien se dispone de ciertos medios tecnológicos, estos no siempre se mantienen actualizados ni, en muchos casos, alcanzan a cubrir la demanda completa, asimismo, es frecuente observar equipos compartidos entre áreas o la ausencia de mantenimiento preventivo, lo que, en conjunto, limita el rendimiento y la continuidad de las operaciones.

c) **Niveles 0 y 1 (13.3 %):** Se detectaron algunas carencias significativas en la asignación de recursos tecnológicos, estas limitaciones, que afectan tanto la infraestructura como las licencias de software y están comprometidas la eficiencia del proceso de reclutamiento debido a que el acceso a soporte especializado se incrementa los riesgos operativos y se dificulta la implementación de mejoras sostenidas en el tiempo.

En la Fig. 13 se muestra la respuesta a la pregunta 5: *¿El personal recibe capacitación para utilizar de forma segura los sistemas informáticos?*

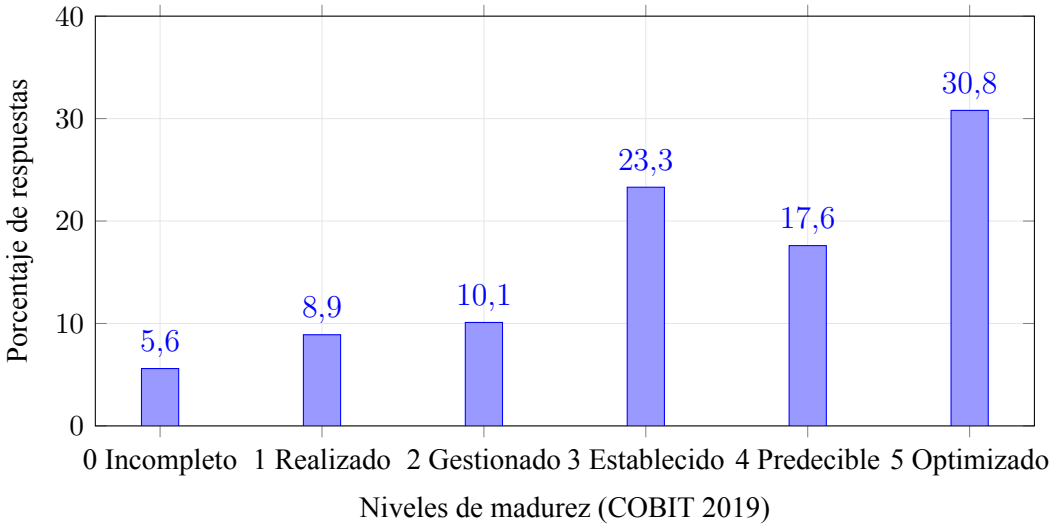

Fig. 13. Google Forms: ¿El personal recibe capacitación para utilizar de forma segura los sistemas informáticos?

Distribución de respuestas:

- 5.6 % en el nivel 0 – Incompleto.
- 8.9 % en el nivel 1 – Realizado.
- 10.1 % en el nivel 2 – Gestionado.
- 23.3 % en el nivel 3 – Establecido.
- 17.6 % en el nivel 4 – Predecible.
- 30.8 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (48.4 %):** La institución tiene programas regulares de capacitación esto fortalecen la seguridad informática y promueven prácticas responsables del personal en el uso de los sistemas.

b) **Niveles 2 y 3 (33.4 %):** Se observan iniciativas que las realizan de vez en cuando, careciendo de continuidad y estandarización, dichas actividades responden a la necesidad inmediata y la disponibilidad circunstancial en las área de tecnológica, que no tienen una planificación anual consolidada.

c) **Niveles 0 y 1 (14.5 %):** Una parte del personal manifiesta no recibir capacitación adecuada para operar los sistemas informáticos con los niveles de seguridad requeridos.

En la Fig. 14 se muestra la respuesta a la pregunta 6: *¿Están claramente definidos los roles y responsabilidades en el uso de los sistemas de reclutamiento?*

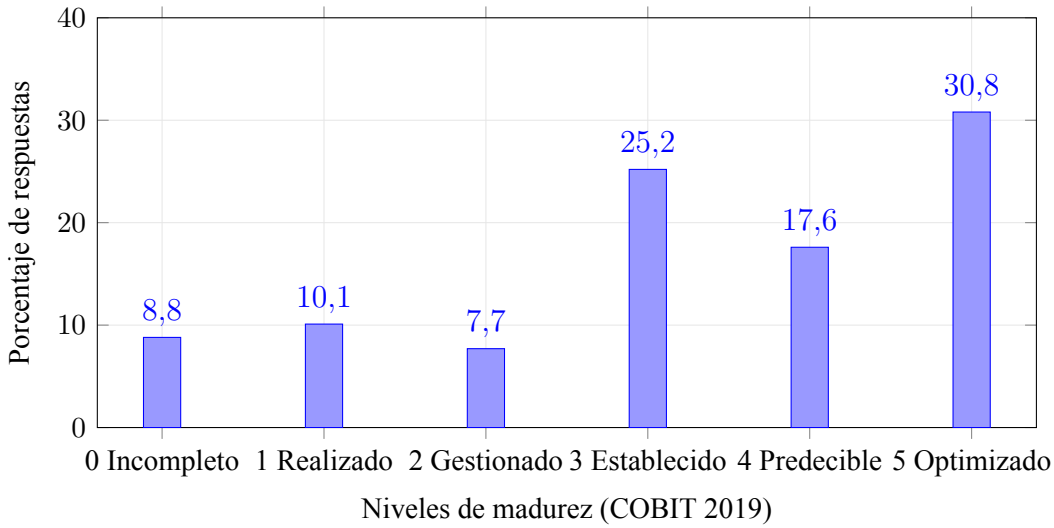

Fig. 14. Google Forms: ¿Están claramente definidos los roles y responsabilidades en el uso de los sistemas de reclutamiento?

Distribución de respuestas:

- 8.8 % en el nivel 0 – Incompleto.
- 10.1 % en el nivel 1 – Realizado.
- 7.7 % en el nivel 2 – Gestionado.
- 25.2 % en el nivel 3 – Establecido.
- 17.6 % en el nivel 4 – Predecible.

- 30.8 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (48.4 %):** La institución ha establecido una distribución clara de funciones para el uso de los sistemas de reclutamiento, además, los roles aparecen debidamente documentados y alineados con los procedimientos internos, lo que, en consecuencia, garantiza una segregación adecuada de tareas y previene duplicidades o conflictos de autoridad, asimismo, esta claridad funcional contribuye a una gestión más controlada y coherente del proceso.

b) **Niveles 2 y 3 (32.9 %):** La estructura funcional se encuentra parcialmente definida, si bien existen responsabilidades asignadas, estas no siempre cuentan con documentación formal ni, en algunos casos, aparecen actualizadas en los manuales de procesos, por ello, persisten vacíos que dificultan la estandarización operativa y pueden generar interpretaciones ambiguas sobre las funciones que debe cumplir cada puesto.

c) **Niveles 0 y 1 (18.9 %):** La carencia de una taxonomía formal de perfiles de usuario vinculados a los activos de información compromete la integridad sistémica; esta ambigüedad estructural detona fricciones en el flujo operativo, errores de aserción en el input de datos y una erosión en la trazabilidad para el deslinde de responsabilidades técnicas.

En la Fig. 15 se muestra la respuesta a la pregunta 7: ¿El software de reclutamiento es actualizado periódicamente considerando estándares de seguridad?

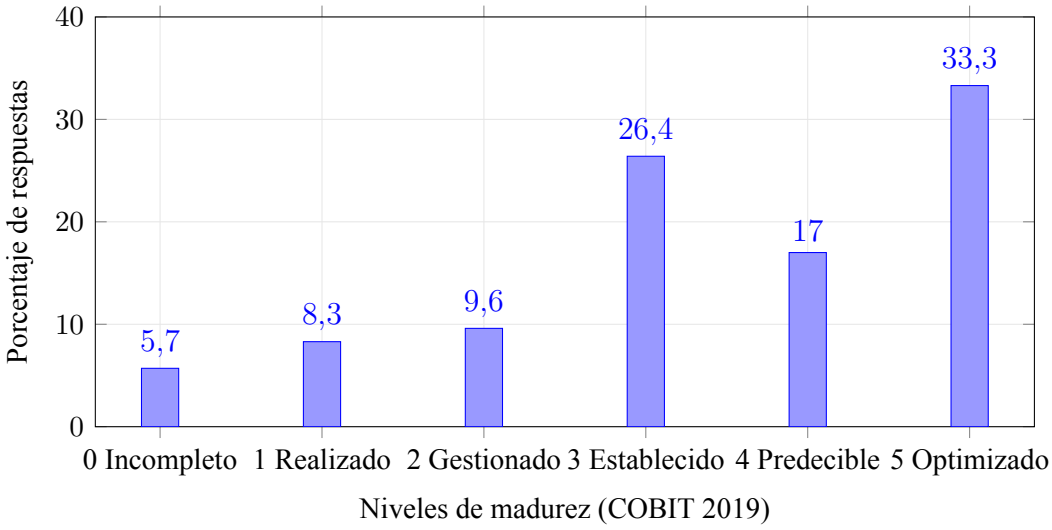

Fig. 15. Google Forms: ¿El software de reclutamiento es actualizado periódicamente considerando estándares de seguridad?

Distribución de respuestas:

- 5.7 % en el nivel 0 – Incompleto.

- 8.3 % en el nivel 1 – Realizado.
- 9.6 % en el nivel 2 – Gestionado.
- 26.4 % en el nivel 3 – Establecido.
- 17.0 % en el nivel 4 – Predecible.
- 33.3 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (50.3 %):** La institución mantiene un proceso formal para actualizar el software de reclutamiento y, además, prioriza el cumplimiento de estándares de seguridad y las mejores prácticas de mantenimiento, de esta manera, se asegura que las plataformas tecnológicas operen bajo condiciones óptimas y reduzcan los riesgos asociados a vulnerabilidades o fallos funcionales. Asimismo, este nivel de control refleja una gestión madura y orientada a la mejora continua.

b) **Niveles 2 y 3 (36.0 %):** Las actualizaciones se realizan de manera irregular, sin una programación establecida ni, en muchos casos, una documentación consistente que permita dar seguimiento adecuado, como resultado, la gestión depende con frecuencia de proveedores externos o, en su defecto, enfrenta limitaciones técnicas que dificultan el control y la evaluación de las mejoras implementadas. Por ello, persisten brechas que impiden alcanzar un nivel de madurez más robusto en la administración del software.

c) **Niveles 0 y 1 (14.0 %):** Evidencian que en ciertos casos no se llevan a cabo actualizaciones regulares o que los procesos de mantenimiento son reactivos ante fallos detectados esto genera vulnerabilidades en la infraestructura tecnológica y un mayor riesgo de exposición ante incidentes de seguridad.

En la Fig. 16 se muestra la respuesta a la pregunta 8: ¿Antes de implementar cambios en el sistema, se realizan evaluaciones de seguridad?

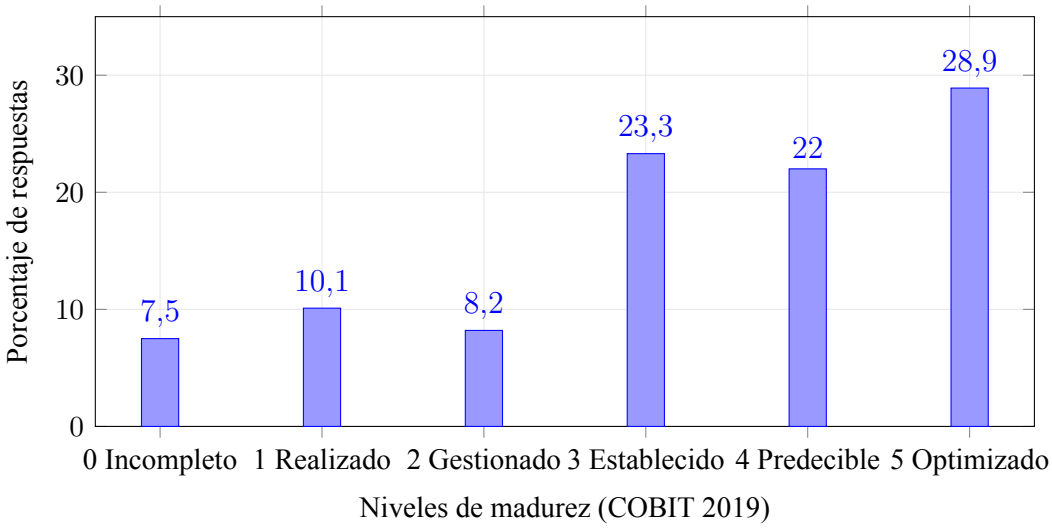

Fig. 16. Google Forms: ¿Antes de implementar cambios en el sistema, se realizan evaluaciones de seguridad?

Distribución de respuestas:

- 7.5 % en el nivel 0 – Incompleto.
- 10.1 % en el nivel 1 – Realizado.
- 8.2 % en el nivel 2 – Gestionado.
- 23.3 % en el nivel 3 – Establecido.
- 22.0 % en el nivel 4 – Predecible.
- 28.9 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (50.9 %):** El área de tecnológica realiza evaluaciones previas a la implementación de cambios en los sistemas y donde se llevan acabo de forma estructurada y alineada con las buenas prácticas de gestión, de este modo, se reducir la probabilidad de errores y garantiza que las modificaciones sean integradas de manera controlada.

b) **Niveles 2 y 3 (31.5 %):** Reflejan que existen procesos de revisión, aunque estos no siempre se aplican de manera sistemática, en efecto, en algunos casos los cambios pueden ejecutarse sin una evaluación formal de riesgos, lo cual, a su vez, limita la detección oportuna de vulnerabilidades y dificulta un control adecuado sobre los impactos que podrían generarse, por consiguiente, la falta de estandarización en estas prácticas deja espacio para inconsistencias y riesgos operativos.

c) **Niveles 0 y 1 (17.6 %):** Demuestran que en ciertos escenarios los cambios se realizan de forma reactiva o improvisada, sin considerar su impacto en la seguridad del sistema, esta práctica incrementa la posibilidad de errores técnicos, brechas de seguridad o pérdida temporal de servicios.

En la Fig. 17 se muestra la respuesta a la pregunta 9: ¿Se efectúan pruebas antes de poner en producción nuevas aplicaciones o actualizaciones?

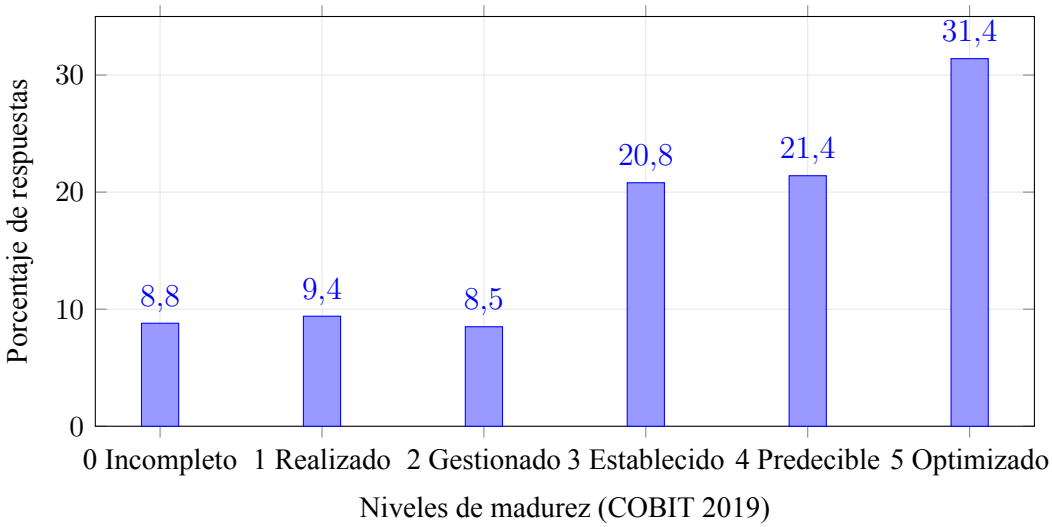

Fig. 17. Google Forms: ¿Se efectúan pruebas antes de poner en producción nuevas aplicaciones o actualizaciones?

Distribución de respuestas:

- 8.8 % en el nivel 0 – Incompleto.
- 9.4 % en el nivel 1 – Realizado.
- 8.5 % en el nivel 2 – Gestionado.
- 20.8 % en el nivel 3 – Establecido.
- 21.4 % en el nivel 4 – Predecible.
- 31.4 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (52.8 %):** La mayoría del personal esta de acuerdo con que hay un proceso estructurado de pruebas antes de implementar nuevas aplicaciones, este esquema incorpora entornos de prueba específicos, revisiones de seguridad y verificaciones funcionales que garantizan la calidad y estabilidad del software desplegado.

b) **Niveles 2 y 3 (29.3 %):** La inexistencia de protocolos institucionalizados evidencia una praxis técnica centrada en requerimientos funcionales elementales; sistemáticamente, se omiten auditorías de seguridad perimetral y análisis de estrés sobre el rendimiento del backend.

c) **Niveles 0 y 1 (18.2 %):** Esta métrica refleja una carencia crítica en la gobernanza de TI, donde la ausencia de entornos de staging formalizados imposibilita la validación de integridad previa al despliegue en producción.

En la Fig. 18 se muestra la respuesta a la pregunta 10: ¿El acceso a la información sensible de los aspirantes está controlado y limitado al personal autorizado? Este ítem permite evaluar las prácticas de control de acceso y confidencialidad en el manejo de los datos personales dentro del proceso de reclutamiento.

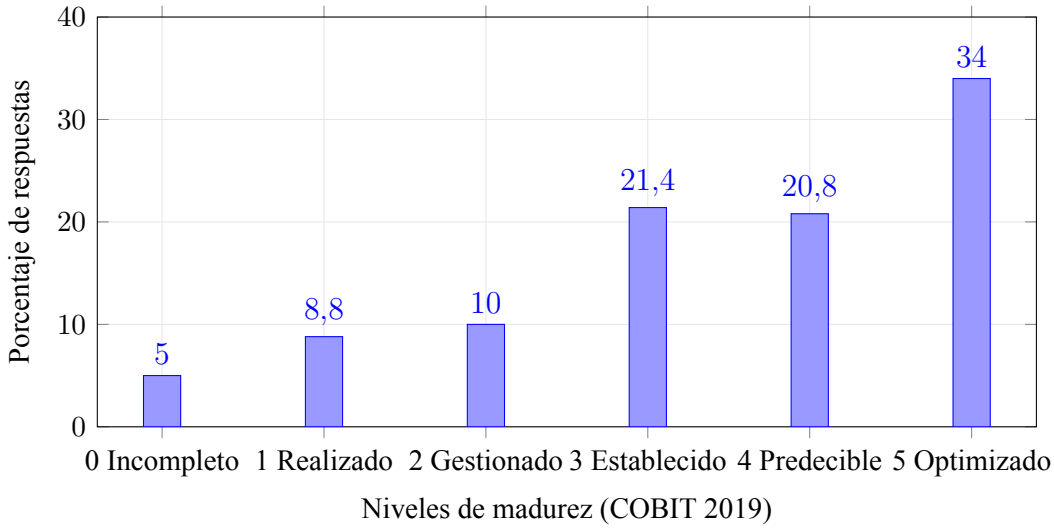

Fig. 18. Google Forms: ¿El acceso a la información sensible de los aspirantes está controlado y limitado al personal autorizado?

Distribución de respuestas:

- 5.0 % en el nivel 0 – Incompleto.
- 8.8 % en el nivel 1 – Realizado.
- 10.0 % en el nivel 2 – Gestionado.
- 21.4 % en el nivel 3 – Establecido.
- 20.8 % en el nivel 4 – Predecible.
- 34.0 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (54.8 %):** SE observa que más de la mitad de los participantes considera que si existen mecanismos formales para controlar el acceso a la información confidencial, dichos roles incluyen la autenticación por usuario, roles diferenciados, registros de auditoría y la restricciones basadas en permisos, lo que contribuye al cumplimiento de la ley orgánica de protección de datos personales.

b) **Niveles 2 y 3 (31.4 %):** Las políticas de acceso existen, aunque su aplicación resulta inconsistente y carece de supervisión permanente. El control depende principalmente de la confianza depositada en el personal o de prácticas operativas establecidas, sin contar con sistemas automatizados que verifiquen técnicamente el cumplimiento.

c) **Niveles 0 y 1 (13.8 %):** Muestran que aún existen áreas en las que los datos personales pueden ser accedidos sin las medidas adecuadas de restricción.

En la Fig. 19 se muestra la respuesta a la pregunta 11: ¿El sistema cuenta con respaldo y recuperación confiable en caso de fallas?

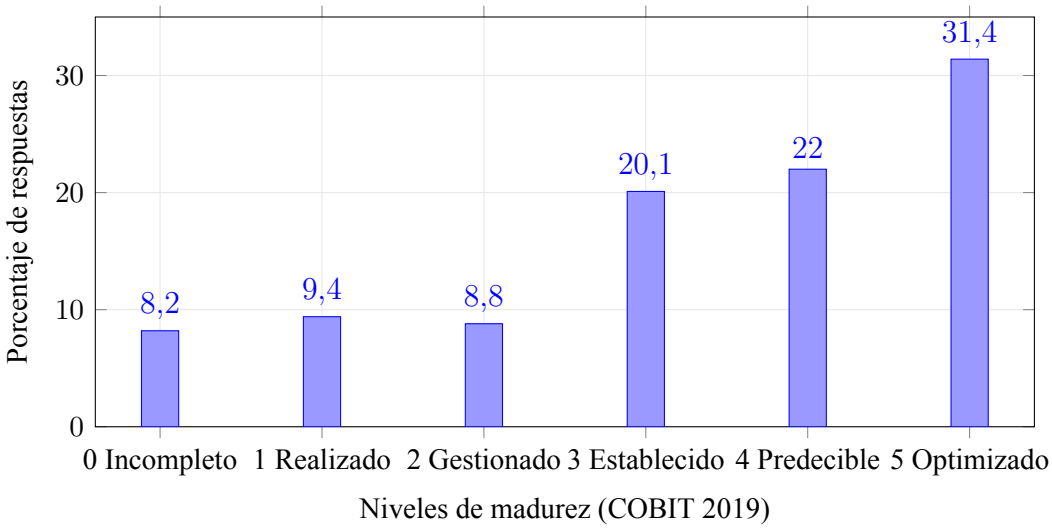

Fig. 19. Google Forms: ¿El sistema cuenta con respaldo y recuperación confiable en caso de fallas?

Distribución de respuestas:

- 8.2 % en el nivel 0 – Incompleto.
- 9.4 % en el nivel 1 – Realizado.
- 8.8 % en el nivel 2 – Gestionado.
- 20.1 % en el nivel 3 – Establecido.

- 22.0 % en el nivel 4 – Predecible.
- 31.4 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (53.4 %):** Los resultados obtenidos en la encuesta demostraron que una parte de los encuestados siendo un número significativo considerarón que si existen mecanismos sólidos de respaldo y la recuperación ante fallas localizadas.

b) **Niveles 2 y 3 (28.9 %):** Indican que, si bien existen políticas de respaldo, su aplicación podría no ser constante o carecer de pruebas regulares de recuperación.

c) **Niveles 0 y 1 (17.6 %):** Reflejan que ciertos procesos aún no disponen de un esquema formal de respaldo o dependen de acciones manuales no verificadas.

En la Fig. 20 se presenta la respuesta a la pregunta 12: ¿El soporte técnico atiende oportunamente los incidentes relacionados con el proceso de reclutamiento?

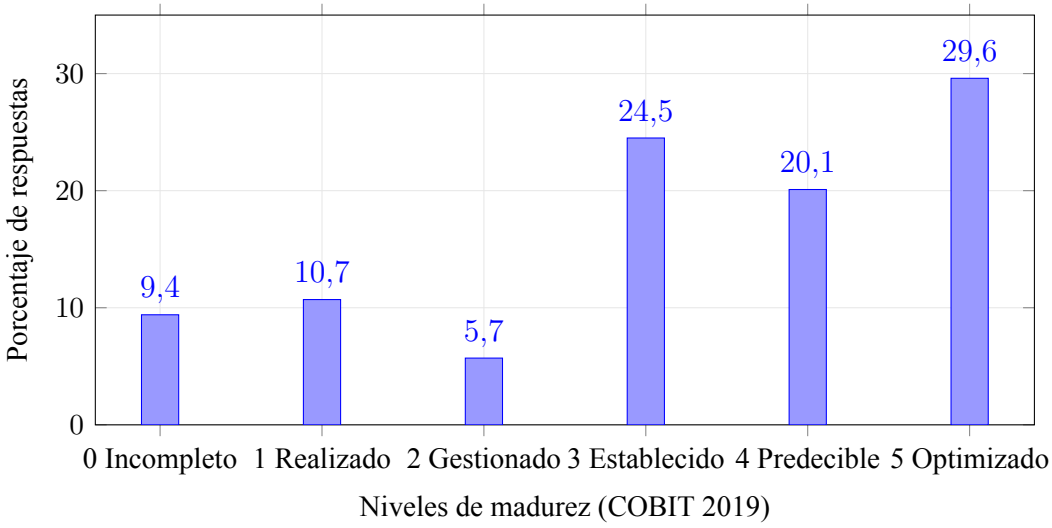

Fig. 20. Google Forms: ¿El soporte técnico atiende oportunamente los incidentes relacionados con el proceso de reclutamiento?

Distribución de respuestas:

- 9.4 % en el nivel 0 – Incompleto.
- 10.7 % en el nivel 1 – Realizado.
- 5.7 % en el nivel 2 – Gestionado.
- 24.5 % en el nivel 3 – Establecido.

- 20.1 % en el nivel 4 – Predecible.
- 29.6 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (49.7 %):** Se pudo observar que casi la mitad de los encuestados estaban de acuerdo en que el soporte técnico brinda atención eficiente y oportuna ante cualquier incidentes que este relacionado con el sistema de reclutamiento.

b) **Niveles 2 y 3 (30.2 %):** El soporte técnico se proporciona, aunque opera sin una estructura completamente definida que garantice su eficacia.

c) **Niveles 0 y 1 (20.1 %):** Hay Persistencia de dificultades significativas para atender incidentes de manera oportuna.

En la Fig. 21 se presentan los resultados de la pregunta 13: ¿Se miden indicadores de desempeño de los sistemas de reclutamiento?

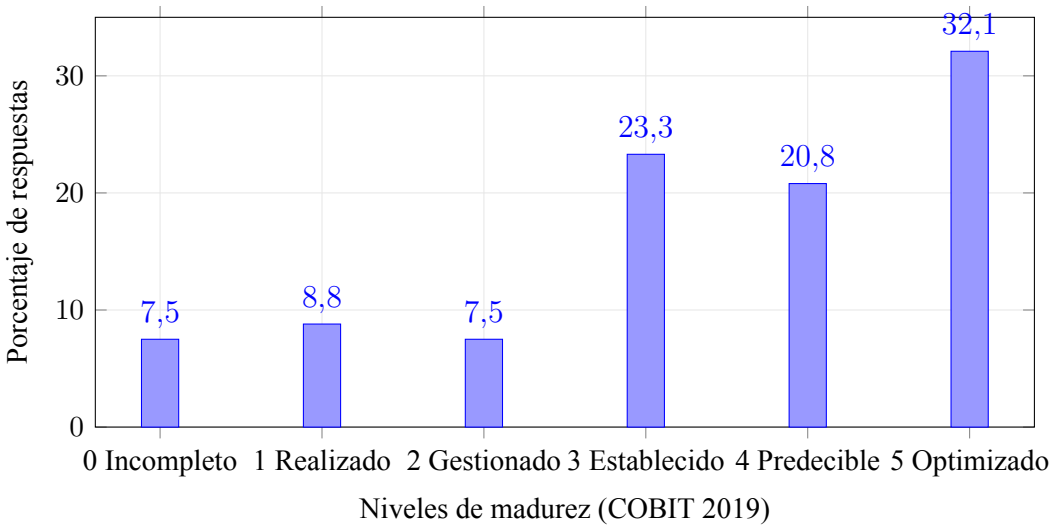

Fig. 21. Google Forms: ¿Se miden indicadores de desempeño de los sistemas de reclutamiento?

Distribución de respuestas:

- 7.5 % en el nivel 0 – Incompleto.
- 8.8 % en el nivel 1 – Realizado.
- 7.5 % en el nivel 2 – Gestionado.
- 23.3 % en el nivel 3 – Establecido.
- 20.8 % en el nivel 4 – Predecible.

- 32.1 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (52.9 %):** Los resultados demuestran que la mayoría de los encuestados admiten que hay mecanismos consolidados para medir el desempeño del sistema de reclutamiento, de esta manera estos incluyen métricas como tiempos de respuesta, efectividad de los filtros de selección y disponibilidad del sistema, evidenciando un proceso de evaluación estructurado y continuo.

b) **Niveles 2 y 3 (30.8 %):** Algunas áreas utilizan indicadores específicos, aunque estos no se alinean completamente con los objetivos estratégicos del departamento de TI. Tampoco se realiza un análisis periódico de los resultados obtenidos.

c) **Niveles 0 y 1 (16.3 %):** Se determinó que existe procesos que carecen de indicadores formales y no se cuentan con mecanismos de control establecidos.

En la Fig. 22 se muestran los resultados de la pregunta 14: ¿Se realizan auditorías internas o externas de los procesos de TI en el área de talento humano?

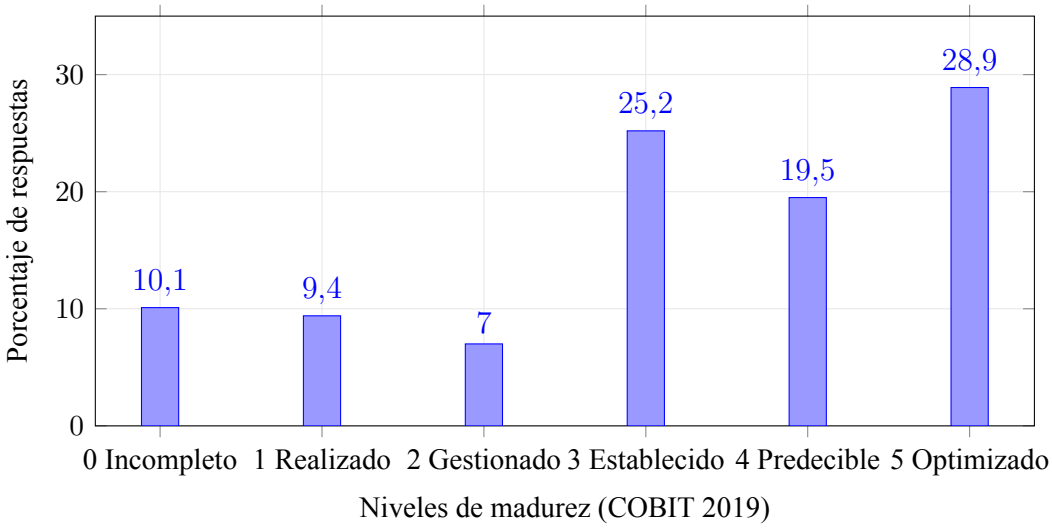

Fig. 22. Google Forms: ¿Se realizan auditorías internas o externas de los procesos de TI en el área de talento humano?

Distribución de respuestas:

- 10.1 % en el nivel 0 – Incompleto.
- 9.4 % en el nivel 1 – Realizado.
- 7.0 % en el nivel 2 – Gestionado.

- 25.2 % en el nivel 3 – Establecido.
- 19.5 % en el nivel 4 – Predecible.
- 28.9 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (48.4 %):** Los resultados obtenidos en la encuesta muestran que los nivel de cumplimiento refiriéndose a la ejecución de auditorías internas o externas están en estandares altos.

b) **Niveles 2 y 3 (32.2 %):** Indican que algunas organizaciones realizan auditorías de manera parcial o con una frecuencia no establecida.

c) **Niveles 0 y 1 (19.5 %):** Reflejan la ausencia de procesos formales de auditoría o la falta de registros documentados sobre su realización.

En la Fig. 23 se presentan los resultados de la pregunta 15: ¿Se evalúan regularmente los resultados de las medidas de seguridad implementadas?

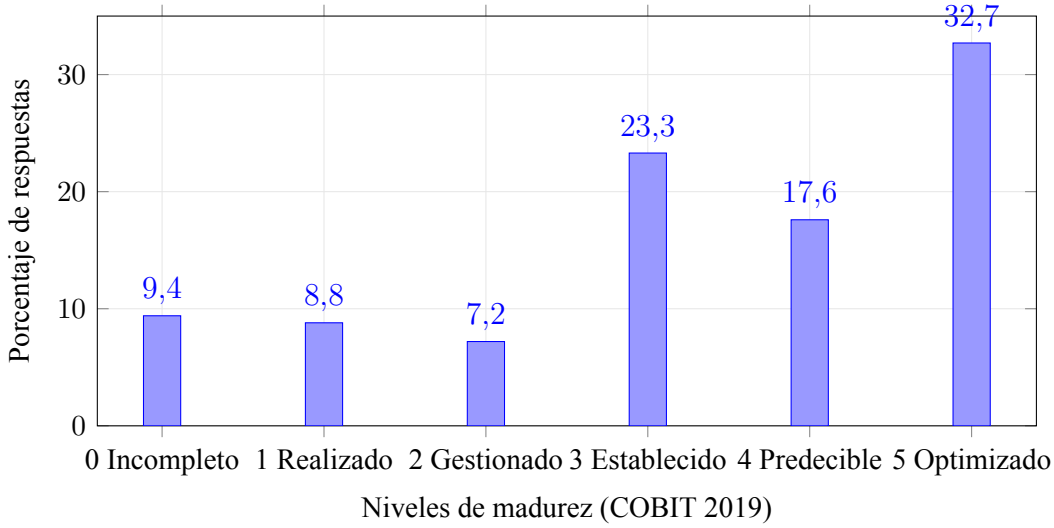

Fig. 23. Google Forms: ¿Se evalúan regularmente los resultados de las medidas de seguridad implementadas?

Distribución de respuestas:

- 9.4 % en el nivel 0 – Incompleto.
- 8.8 % en el nivel 1 – Realizado.
- 7.2 % en el nivel 2 – Gestionado.
- 23.3 % en el nivel 3 – Establecido.

- 17.6 % en el nivel 4 – Predecible.
- 32.7 % en el nivel 5 – Optimizado.

Interpretación:

a) **Niveles 4 y 5 (50.3 %):** Los datos revelan que un segmento mayoritario percibe una cadencia sistemática en la auditoría de controles; este grupo ratifica la operatividad de frameworks para la telemetría de resultados, la gestión documental de informes técnicos y la implementación de acciones correctivas derivadas de la detección de vulnerabilidades.

b) **Niveles 2 y 3 (30.5 %):** Se realizan revisiones parciales que carecen de una sistemática definida.

c) **Niveles 0 y 1 (18.2 %):** Existen numerosos procesos que operan sin evaluar la efectividad real de las medidas de seguridad.

El análisis arrojó los siguientes valores promedio por dominio, los cuales reflejan el nivel de madurez alcanzado en el departamento de talento humano del GIR bajo el marco de referencia Cobit 2019. Como se observa en la Tabla IV, los valores se encuentran en un rango intermedio, con mayor fortaleza en el dominio EDM y debilidades relativas en el dominio APO.

Tabla IV.
CÁLCULO DE LA MADUREZ PROMEDIO

Ítem / Dominio	Promedio
Sección A. EDM – Evaluar, Dirigir y Monitorear.	
EDM01: Políticas claras sobre uso de TI en reclutamiento.	3,28
EDM03: Supervisión del cumplimiento de normativas de seguridad.	3,43
EDM04: Identificación y monitoreo de riesgos de TI.	3,42
Promedio EDM	3,42
Sección B. APO – Alinear, Planear y Organizar.	
APO01: Recursos de TI suficientes y adecuados.	3,30
APO12: Capacitación del personal en uso seguro de sistemas.	3,20
APO10: Roles y responsabilidades claramente definidos.	3,28

Continúa en la siguiente página

Continuación de la Tabla IV

Ítem / Dominio	Promedio
Promedio APO	3,26
Sección C. BAI – Construir, Adquirir e Implementar.	
BAI03: Gestión del ciclo de vida y despliegue de actualizaciones en el ecosistema de reclutamiento.	3,38
BAI06: Auditoría de riesgos y controles de seguridad previos a la liberación de cambios en el entorno operativo.	3,31
BAI07: Validación de integridad y pruebas de aceptación del usuario (UAT) antes del aprovisionamiento en producción.	3,32
Promedio BAI	3,34
Sección D. DSS – Entregar, Dar servicio y Soportar.	
DSS05: Control de acceso a información sensible	3,42
DSS04: Respaldo y recuperación confiable en fallas	3,33
DSS02: Atención oportuna de incidentes de TI	3,29
Promedio DSS	3,35
Sección E. MEA – Monitorear, Evaluar y Valorar.	
MEA01: Medición de indicadores de desempeño.	3,38
MEA02: Auditorías internas y externas de TI.	3,24
MEA03: Evaluación de medidas de seguridad.	3,30
Promedio MEA	3,31
Consolidado General	
Promedio Global de Madurez CObit 2019.	3,33

A continuación de detalla el promedio general de cada uno de los dominios, los detalles se encuentran en la Tabla V.

Tabla V.
PROMEDIOS DE MADUREZ POR DOMINIO COBIT 2019

Dominio	Promedio
EDM – Evaluar, Dirigir y Monitorear	3,42
APO – Alinear, Planear y Organizar	3,26
BAI – Construir, Adquirir e Implementar	3,34
DSS – Entregar, Dar Servicio y Soportar	3,35
MEA – Monitorear, Evaluar y Valorar	3,31
Promedio Global	**3,33**

El análisis de los promedios obtenidos por dominio permite identificar fortalezas y debilidades en la gestión de TI del departamento de talento humano del GIR bajo el marco Cobit 2019:

- EDM (3,42): Es el dominio mejor evaluado, lo que indica que existe una percepción favorable respecto al control y supervisión de TI. Sin embargo, la ausencia de políticas documentadas limita que este valor se consolide en un nivel predecible u optimizado.
- **APO (3,26):** El siguiente dominio presentó el promedio más bajo y, en consecuencia de esto se pudo evidenciar las dificultades concretas en la definición de roles, la distribución de recursos y la formación del personal que utilizan el sistema, también, se observó que estas limitaciones afectan la coherencia y continuidad de la gestión operativa.
- **BAI (3,34):** Se observa un desempeño intermedio donde las actualizaciones y las pruebas de software se ejecutan de forma irregular y, en muchos casos, sin una estandarización completa de los procesos, como resultado, persisten inconsistencias que dificultan la consolidación de buenas prácticas técnicas.
- **DSS (3,35):** La gestión de soporte y seguridad se considera adecuada en términos generales; sin embargo, se detectan vulnerabilidades en los mecanismos de respaldo y en los planes de continuidad operativa, asimismo, estas brechas pueden comprometer la estabilidad de los servicios en situaciones críticas.

- **MEA (3,31):** Se identifican carencias significativas en la ejecución de auditorías internas y en el monitoreo de indicadores, lo que limita la capacidad de ajustar y optimizar los procesos de manera sistemática, de igual forma, la falta de seguimiento continuo reduce la eficacia de las acciones correctivas implementadas.

Los resultados estadísticos obtenidos media y desviación estándar por cada ítem se presentan en la Tabla VI, la cual muestra el nivel promedio de madurez percibido y la dispersión de respuestas en cada uno de los criterios evaluados.

Tabla VI.
ENCUESTA COBIT 2019 EN EL GIR (MEDIA Y DESVIACIÓN ESTÁNDAR POR ÍTEM).

Ítem	Media	Desviación estándar
1 ¿Existen políticas claras que regulan el uso de TI en el proceso de reclutamiento GIR?	3.28	1.62
2. ¿La dirección supervisa el cumplimiento de normativas sobre seguridad de datos personales?	3.43	1.50
3. ¿Los riesgos relacionados con TI en reclutamiento son identificados y monitoreados?	3.42	1.57
4. ¿Los recursos de TI asignados al proceso de reclutamiento son suficientes y adecuados?	3.30	1.47
5. ¿El personal recibe capacitación para utilizar de forma segura los sistemas informáticos?	3.20	1.69
6. ¿Están claramente definidos los roles y responsabilidades en el uso de los sistemas de reclutamiento?	3.28	1.59
7. ¿El software de reclutamiento es actualizado periódicamente considerando estándares de seguridad?	3.38	1.55
8. ¿Antes de implementar cambios en el sistema, se realizan evaluaciones de seguridad?	3.31	1.55

Continúa en la siguiente página

Continuación de la Tabla VI

Ítem	Media	Desviación estándar
9. ¿Se efectúan pruebas antes de poner en producción nuevas aplicaciones o actualizaciones?	3.32	1.61
10. ¿El acceso a la información sensible de los aspirantes está controlado y limitado al personal autorizado?	3.42	1.57
11. ¿El sistema cuenta con respaldo y recuperación confiable en caso de fallas?	3.33	1.61
12. ¿El soporte técnico atiende oportunamente los incidentes relacionados con el proceso de reclutamiento?	3.29	1.58
13. ¿Se miden indicadores de desempeño de los sistemas de reclutamiento?	3.38	1.56
14. ¿Se realizan auditorías internas o externas de los procesos de TI en el área de talento humano?	3.24	1.61
15. ¿Se evalúan regularmente los resultados de las medidas de seguridad implementadas?	3.30	1.64

Comparación de los niveles de madurez.

Con el propósito de identificar las brechas existentes entre la situación actual del departamento de talento humano del GIR y los objetivos de madurez definidos por el marco Cobit 2019, se elaboró una tabla comparativa, en ella se presentan los niveles de madurez obtenidos a partir del análisis estadístico y los niveles objetivos establecidos en la escala de 0 a 5 de Cobit 2019.

Tal como se muestra en la Tabla VII, los resultados evidencian que, aunque los procesos evaluados se encuentran en un nivel establecido, el objetivo es avanzar hacia un nivel predecible, lo que implica fortalecer la estandarización, el control y la mejora continua en cada uno de los dominios.

Tabla VII.
COMPARACIÓN DE NIVELES DE MADUREZ OBTENIDOS VS. NIVELES OBJETIVOS SEGÚN COBIT 2019

Dominio	Nivel obtenido	Nivel objetivo (COBIT 2019)
EDM – Evaluar, Dirigir y Monitorear	3,42 (Establecido)	4 (Predecible)
APO – Alinear, Planear y Organizar	3,26 (Establecido)	4 (Predecible)
BAI – Construir, Adquirir e Implementar	3,34 (Establecido)	4 (Predecible)
DSS – Entregar, Dar Servicio y Soportar	3,35 (Establecido)	4 (Predecible)
MEA – Monitorear, Evaluar y Valorar	3,31 (Establecido)	4 (Predecible)
Promedio Global	**3,33 (Establecido)**	**4 (Predecible)**

Comparación gráfica de niveles de madurez.

Para complementar el análisis estadístico, se presenta un gráfico comparativo de los niveles de madurez obtenidos en la encuesta frente a los niveles objetivos definidos en COBIT 2019, de esta manera, este recurso visual permite identificar claramente las brechas existentes en cada dominio y, además, facilita la priorización de acciones de mejora en la gestión de TI, asimismo, la comparación gráfica ofrece una visión más intuitiva del estado actual, lo que contribuye a una toma de decisiones más informada y estratégica.

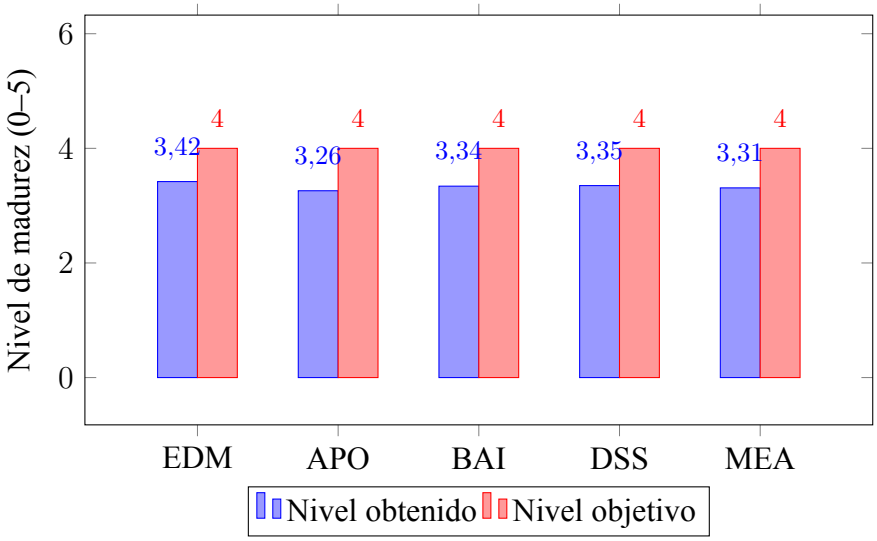

Fig. 24. Comparación de niveles obtenidos y nivel objetivo de madurez (4) por dominio COBIT 2019

Tal como se aprecia en la Fig. 24, los niveles obtenidos en todos los dominios se encuentran en un rango de 3,26 a 3,42, lo que corresponde al nivel establecido, en contraste, el nivel objetivo

definido por COBIT 2019 es de 4 (predecible), esta diferencia evidencia brechas que deben cerrarse, en particular en los dominios APO y MEA, que presentan los valores más bajos.

Brecha entre niveles obtenidos y objetivos.

Para comprender la distancia entre la situación actual y el nivel deseado, se calcularon las brechas entre los valores de madurez recogidos en la encuesta y el nivel 4 de COBIT 2019 —el estándar predecible que se busca alcanzar. de esta manera, la Tabla VIII sintetiza estos hallazgos y señala con claridad los dominios que requieren una atención prioritaria, en particular, APO y MEA destacan con las diferencias más amplias, lo cual revela carencias importantes en la planificación estratégica, la asignación de recursos, la capacitación del personal y, además, en los procesos de auditoría interna, en consecuencia, estos resultados orientan la necesidad de fortalecer dichos ámbitos para avanzar hacia un modelo de gestión más maduro y alineado con las buenas prácticas del marco COBIT 2019.

Tabla VIII.
BRECHA ENTRE NIVELES OBTENIDOS Y NIVELES OBJETIVOS DE MADUREZ SEGÚN COBIT 2019

Dominio	**Nivel obtenido**	**Nivel objetivo (COBIT 2019)**	**Brecha**
EDM – Evaluar, Dirigir y Monitorear	3.42	4.00	0.58
APO – Alinear, Planear y Organizar	3.26	4.00	0.74
BAI – Construir, Adquirir e Implementar	3.34	4.00	0.66
DSS – Entregar, Dar Servicio y Soportar	3.35	4.00	0.65
MEA – Monitorear, Evaluar y Valorar	3.31	4.00	0.69
Promedio Global	**3.33**	**4.00**	**0.67**

Comparación gráfica de niveles de madurez y brechas.

Para visualizar integralmente los resultados de la evaluación, se desarrolló la Fig. 25, una comparación que contrasta los niveles de madurez alcanzados en cada dominio con los objetivos establecidos por COBIT 2019, de este modo, la representación incorpora también las brechas calculadas, lo que permite destacar con claridad aquellas áreas donde la distancia entre la situación actual y el nivel esperado resulta más significativa, asimismo, este enfoque gráfico facilita

la identificación de prioridades y contribuye a orientar la toma de decisiones estratégicas en materia de gestión de TI.

El dominio APO muestra la brecha más amplia (0.74), seguido de cerca por MEA (0.69), ya que estos valores demuestran que hay una necesidad urgente en reforzar los procesos de planificación, la asignación de recursos y auditoría interna y por su parte, EDM presenta una diferencia menor (0.58), indicando un desempeño relativamente más sólido en materia de supervisión y control.

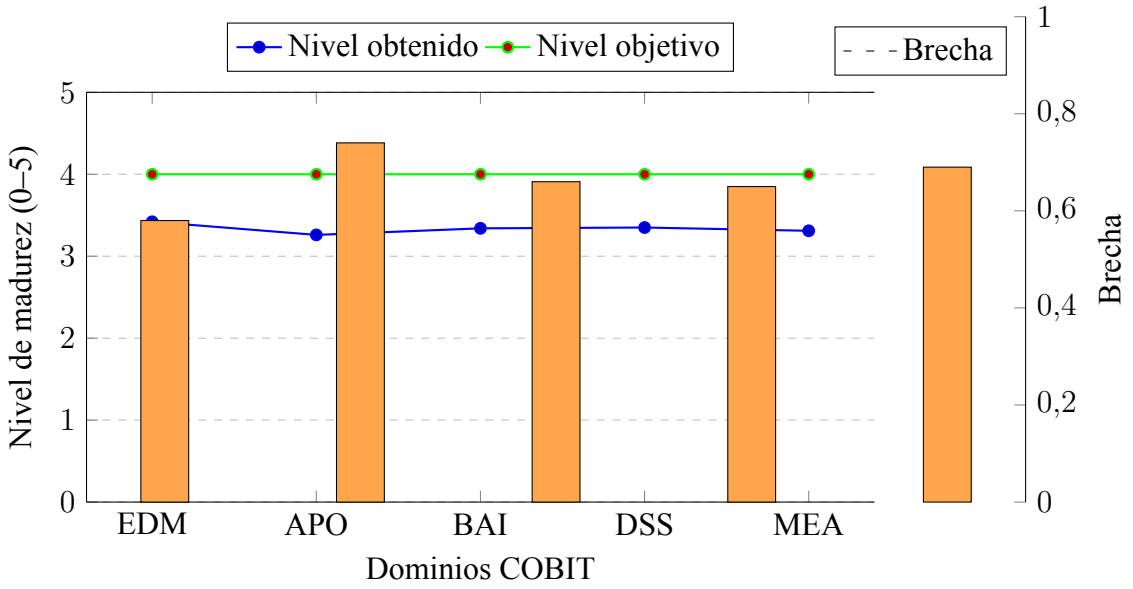

Fig. 25. Brechas, niveles obtenidos y objetivos de madurez por dominio COBIT 2019

Evaluación por dominio.

EDM – Evaluar, Dirigir y Monitorear (3.42 / brecha 0.58) Este dominio obtuvo el mejor desempeño ya que reflejó una percepción favorable sobre los mecanismos de supervisión y control de TI en el GIR, sin embargo, la brecha de 0.58 señala que aún se requiere formalizar políticas documentadas y, además, mediante la estandarizar procesos para alcanzar el nivel "Predecible" (4.0), y de este modo, exista una base sólida que todavía se evidencian oportunidades de mejora en la consolidación de un sistema de gobernanza más estructurado.

APO – Alinear, Planear y Organizar (3.26 / brecha 0.74) Registra la brecha más amplia entre todos los dominios, lo que revela deficiencias críticas en la planificación estratégica, la capacitación del personal y la definición de roles, en consecuencia, urge implementar planes de formación, asignar recursos tecnológicos adecuados y, además, fortalecer la alineación entre los objetivos institucionales y las capacidades de TI, asimismo, este dominio requiere una intervención prioritaria debido al impacto directo que tiene sobre el resto de los procesos organizacionales.

BAI – Construir, Adquirir e Implementar (3.34 / brecha 0.66) Muestra esfuerzos dispersos por actualizar y probar soluciones tecnológicas, aunque sin una metodología uniforme, por ello, la brecha de 0.66 demanda estandarizar los procesos de implementación de cambios, eliminando improvisaciones que puedan afectar la seguridad y la continuidad operativa, adicionalmente, se requiere fortalecer la trazabilidad y la documentación de cada cambio para mejorar la estabilidad del entorno tecnológico.

DSS – Entregar, Dar Servicio y Soportar (3.35 / brecha 0.65) Presenta un nivel aceptable en soporte y gestión de incidentes, no obstante, la brecha de 0.65 expone carencias críticas en los planes de continuidad y en los mecanismos de respaldo de información, representando un riesgo operativo que debe atenderse con prioridad, así, aunque existen prácticas funcionales, la falta de protocolos robustos limita la capacidad de respuesta ante fallos mayores o emergencias.

MEA – Monitorear, Evaluar y Valorar (3.31 / brecha 0.69) En la evaluación de este dominio se determinó debilidades en la realización de auditorías internas y en el uso de indicadores de desempeño, asimismo,existiendo una brecha de 0.69 que confirma los mecanismos de retroalimentación y mejora continua debido a que son insuficientes, impidiendo consolidar un modelo de gobernanza maduro y sostenible, por consiguiente, este dominio requiere fortalecer su estructura de seguimiento para garantizar decisiones más informadas y oportunas.

4.1.3 Resultado de entrevista aplicada.

En la siguiente tabla IX se detalla los resultados obtenidos depués de aplicar la entrevista al personal clave del departamento TI.

Tabla IX.
MATRIZ DE EVALUACIÓN DE CONTROLES BASADA EN COBIT 2019 CON RESULTADOS

Dominio	Control Evaluado (Pregunta)	Criterio de Evaluación	Sí	No	Parcial
EDM01	¿Tenemos políticas que regulen cómo usar la tecnología en los procesos de reclutamiento?	Documentos oficiales que establezcan las reglas para usar sistemas tecnológicos en gestión humana.	✓		

Continúa en la siguiente página

Continuación de la Tabla IX

Dominio	Control Evaluado (Pregunta)	Criterio de Evaluación	Sí	No	Parcial
EDM03	¿Revisamos los riesgos tecnológicos que podrían afectar los datos de los aspirantes?	Informes de auditoría o actas de comités donde se analice esta alineación estratégica.		✗	
EDM04	¿Podemos consultar informes de auditorías anteriores sobre cumplimiento normativo?	Reportes de auditoría que documenten hallazgos previos en riesgos tecnológicos.		✗	
APO01	¿Planificamos los recursos tecnológicos necesarios para apoyar el reclutamiento?	Presupuestos detallados, cronogramas y planes estratégicos de TI debidamente documentados.	✓		
APO10	¿Tenemos claridad sobre quién supervisa los sistemas que nos proporcionan terceros?	Contratos que definan responsabilidades y documentos que asignen roles internos específicos.	✓		
APO12	¿Capacitamos al equipo para identificar y responder a riesgos tecnológicos?	Registros de formación en seguridad, materiales de capacitación y listas de asistencia.	✓		
BAI03	¿Contamos con criterios definidos para seleccionar o actualizar el software de reclutamiento?	Un proceso formal que evalúe costos, funcionalidad y seguridad antes de cualquier decisión.		✗	
BAI06	¿Revisamos los aspectos de seguridad antes de aprobar cambios en los sistemas?	Cada modificación requiere una evaluación de riesgos antes de su autorización.	✓		
BAI07	¿Probamos las herramientas antes de implementarlas definitivamente?	Evidencias de pruebas que verifiquen el funcionamiento, seguridad y rendimiento.	✓		

Continúa en la siguiente página

Continuación de la Tabla IX

Dominio	Control Evaluado (Pregunta)	Criterio de Evaluación	Sí	No	Parcial
DSS05	¿Controlamos quién accede a la información sensible de los candidatos?	Mecanismos de seguridad que autoricen, registren y vigilen los accesos a datos críticos.		✗	
DSS04	¿Sabemos cómo recuperar la información si fallan los sistemas?	Procedimientos documentados de respaldo que se prueben regularmente.		✗	
DSS02	¿El soporte técnico responde a tiempo cuando hay problemas en el reclutamiento?	Incidentes registrados y atendidos según los plazos establecidos en los acuerdos de servicio.	✓		
MEA01	¿Medimos cómo funcionan y qué tan seguros están nuestros sistemas de reclutamiento?	Indicadores de desempeño y métricas de seguridad con seguimiento periódico.	✓		
MEA02	¿Auditamos regularmente los sistemas de reclutamiento?	Auditorías programadas que evalúen la efectividad real de los controles internos.		✗	
MEA03	¿Verificamos si las medidas para reducir riesgos tecnológicos están funcionando?	Análisis que comparen los resultados obtenidos contra los objetivos planteados.			∂

Para representar de manera gráfica los resultados obtenidos en la matriz de evaluación, se elaboró un diagrama de barras que muestra el nivel de cumplimiento de los controles de acuerdo con los dominios de Cobit 2019, este gráfico permite visualizar de manera comparativa las fortalezas y debilidades en cada dominio, evidenciando las áreas en las que la organización cumple plenamente, aquellas en las que existen incumplimientos y los casos donde solo se observó un cumplimiento parcial. Como se muestra en la Fig. 26, el dominio APO presenta el mayor número de controles cumplidos, mientras que en los dominios DSS y MEA se observan más debilidades y hallazgos pendientes de atención.

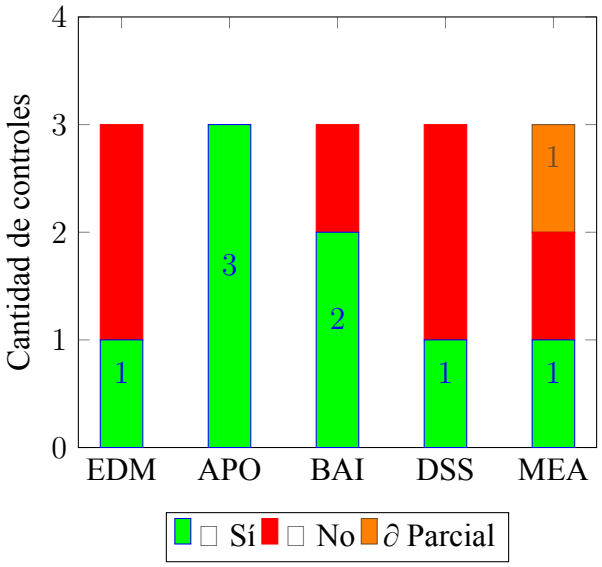

Fig. 26. Brechas, niveles obtenidos y objetivos de madurez por dominio COBIT 2019

El análisis de las respuestas proporcionadas por el departamento de tecnologías de la información, clasificadas dentro de la matriz de evaluación basada en Cobit 2019, permitió identificar tanto las fortalezas como las debilidades y los aspectos parciales en la implementación de los controles, estos hallazgos constituyen un insumo fundamental para el diagnóstico del nivel de madurez institucional en la gobernanza de TI.

Fortalezas.

Se destacan diversas fortalezas que reflejan buenas prácticas consolidadas dentro del área, entre ellas se encuentra la planificación estratégica de TI (APO01), la cual demuestra una adecuada organización en la asignación de recursos tecnológicos para apoyar los procesos institucionales, asimismo se identificó un cumplimiento favorable en la gestión de riesgos (APO12), evidenciando acciones orientadas a la capacitación del personal y a la prevención de incidentes relacionados con la seguridad informática.

Otro aspecto positivo corresponde a la gestión de proveedores (APO10), donde se cuenta con roles y responsabilidades claramente establecidos para la supervisión de servicios externos, especialmente vinculados con el software utilizado en los procesos, en cuanto a la implementación tecnológica, se destaca la evaluación de seguridad en cambios de software (BAI06), en la que se verifican los posibles riesgos antes de introducir modificaciones, y finalmente la gestión de incidentes (DSS02), que demuestra tiempos de respuesta oportunos frente a problemas técnicos que afectan el desarrollo de las actividades.

Debilidades.

El análisis reveló importantes debilidades que requieren atención prioritaria, en lo relacionado con el cumplimiento normativo (EDM03, EDM04), no se encontraron mecanismos formales que aseguren la supervisión de disposiciones legales, especialmente en materia de datos personales, lo que genera un riesgo de incumplimiento frente a normativas vigentes.

La continuidad del servicio (DSS04) no cuenta con planes de respaldo y recuperación documentados, lo que podría comprometer la estabilidad de los procesos en caso de incidentes graves, en la seguridad de la información (DSS05) se identificó la ausencia de controles efectivos para restringir y monitorear los accesos a información sensible de aspirantes, lo cual representa un riesgo significativo de confidencialidad.

No evidenciamos la existencia de procesos formales, internos o externos, que evalúen periódicamente el desempeño de los sistemas de información limitando así la capacidad de detección temprana de vulnerabilidades.

Aspecto parcial.

Existen aspectos parcialmente ejecutados para mitigar riesgos específicamente en MEA03, ya que si bien se aplican acciones correctivas, notamos que carecen de documentación adecuada y no están vinculadas a indicadores que midan objetivamente su efectividad, de este modo la situación revela la necesidad urgente de estandarizar los procesos y formalizar la evidencia que respalde cada medida implementada.

Los resultados preliminares indicaron que hay un avance significativo en aspectos operativos y de planificación dentro de la organización, no obstante, persisten brechas críticas en seguridad, cumplimiento normativo y continuidad de los servicios, teniendo en conjunto, estos hallazgos constituyen el cimiento para desarrollar un plan de mejora que fortalezca la gobernanza de TI, alineado con los lineamientos de COBIT 2019.

4.1.4 Resultados del análisis de la matriz Cobit 2019.

El análisis de la matriz de evaluación aplicada con COBIT 2019 nos entregó datos cuantitativos y cualitativos que retratan fielmente el estado actual de la gobernanza tecnológica en la organización. Estos son los hallazgos que obtuvimos.

Datos Cuantitativos.

En total se evaluaron 15 controles, de los cuales 7 cumplen adecuadamente, 7 no cumplen y 1 se encuentra parcialmente implementado. Esto corresponde a un 46.7 % de cumplimiento, 46.7 % de no cumplimiento y 6.6 % de cumplimiento parcial como se observa en la Tabla X .

Tabla X.
CUMPLIMIENTO POR DOMINIO COBIT 2019

Dominio	**Total controles**	**Cumple (✓)**	**No cumple (✗)**	**Parcial (∂)**	**% Cumplimiento**
EDM	3	1	2	0	33.3 %
APO	3	3	0	0	100 %
BAI	3	2	1	0	66.7 %
DSS	3	1	2	0	33.3 %
MEA	3	1	1	1	33.3 %

Se observa que el dominio con mejor desempeño es *APO*, que alcanza el 100 % de cumplimiento, mientras que los dominios con menor desempeño son *EDM*, *DSS* y *MEA*, con apenas un 33.3 % de cumplimiento.

Datos Cualitativos.

Los resultados nos permitieron reconocer las fortalezas, debilidades y aquellos aspectos que requieren mayor desarrollo en la aplicación de controles de tecnología.

- **Fortalezas (✓).** Identificamos varios puntos sólidos en la gestión actual la planificación estratégica demuestra una organización adecuada para asignar recursos tecnológicos en gestión de riesgos, existen capacitaciones y medidas preventivas frente a incidentes de seguridad los roles y responsabilidades con proveedores externos están claramente definidos los cambios de software incluyen evaluaciones de seguridad antes de su implementación y se realizan pruebas de aceptación antes de pasar a producción, el área de soporte responde con tiempos oportunos a los incidentes reportados y se realiza un seguimiento constante de los indicadores de desempeño tecnológico.

- **Debilidades (✗).**

  Detectamos varios aspectos críticos que necesitan atención inmediata no existen mecanismos formales para supervisar el cumplimiento normativo la selección de software carece de criterios documentados que guíen la evaluación, la seguridad de la información presenta vacíos importantes en los controles de acceso a datos sensibles y no contamos con

planes definidos para respaldo y recuperación ante contingencias. No se realizan auditorías periódicas que verifiquen los controles establecidos.

- **Aspectos Parciales (∂)** La evaluación de medidas para mitigar riesgos muestra un avance limitado si bien se implementan algunas acciones correctivas, estas se aplican de manera informal sin documentación adecuada ni indicadores que permitan medir su efectividad real.

Los resultados muestran que la organización presenta un nivel de madurez intermedio en la gobernanza de TI, existen fortalezas claras en los procesos de planificación, gestión de riesgos y operaciones técnicas; sin embargo también se evidencian debilidades críticas relacionadas con seguridad, cumplimiento normativo y continuidad del servicio, los aspectos parciales identificados reflejan procesos en transición que requieren formalización y estandarización. Estos hallazgos nos servirán para que la propuesta del plan de acción permita cerrar brechas y fortalecer la gobernanza de TI.

4.1.5 Resultado de pruebas técnicas – escaneo Nmap general.

Los resultados generales evidencian que los tres departamentos operan bajo sistemas Microsoft Windows, con protocolos y servicios habilitados en red local, sin políticas estrictas de control de acceso, ni mecanismos formales de auditoría o cifrado de comunicaciones, los hallazgos muestran que los puertos 135 (Microsoft RPC), 139 (NetBIOS-SSN), 445 (Microsoft-DS) y 5357 (HTTP Microsoft HTTPAPI 2.0) permanecen abiertos de forma persistente, lo cual representa una amenaza común de exposición de servicios internos, además se detectaron instancias de software remoto como AnyDesk, que podrían ser utilizados para accesos no autorizados si no se implementan medidas de autenticación y monitoreo adecuado.

De acuerdo con el marco de referencia Cobit 2019, las vulnerabilidades detectadas se relacionan principalmente con los dominios EDM04 (Optimización del riesgo), APO12 (Gestión de riesgos), DSS05 (Gestión de la seguridad de los servicios) y MEA02 (Evaluación del control interno), el análisis integral demuestra la necesidad de fortalecer los controles técnicos, la supervisión continua y la documentación formal de políticas de seguridad, con el fin de garantizar la protección de la información crítica y el cumplimiento normativo institucional.

Escaneo Nmap al departamento de talento humano

Para comenzar, se realizó un escaneo técnico detallado de la red y de los sistemas pertenecientes al departamento de talento humano, con el fin de evaluar los servicios activos y, además, identificar posibles vulnerabilidades en los equipos que gestionan la información del personal postulante.

Durante esta revisión, encontramos algunos puertos abiertos que requieren mayor atención, entre ellos: 135 para Microsoft RPC, 139 con NetBIOS-SSN, 445 para Microsoft-DS, 554 de RTSP, 2869 y 5357 asociados a HTTP Microsoft HTTPAPI 2.0, 7070 utilizado por AnyDesk SSL y 10243 correspondiente a servicios HTTP SSDP/UPnP, es asi como, estos puertos están expuestos que permiten inferir la presencia de servicios internos que podrían ser susceptibles a ataques si no cuentan con los controles adecuados.

Por otra parte, el sistema operativo ha detectado corresponde a Microsoft Windows, con servicios SMB, NetBIOS y HTTP actualmente activos, además, identificamos que el servicio AnyDesk Client se encuentra operando con un certificado válido, pero sin autenticación multifactor configurada, lo que puede incrementar el riesgo de accesos indebidos.

Este análisis muestra la clara exposición de servicios críticos vinculados tanto a la transferencia de archivos como al control remoto, escenarios donde los mecanismos de autenticación resultan insuficientes y como consecuencia, los principales riesgos identificados incluyen accesos no autorizados, existiendo pérdida potencial de información y propagación de malware a través de la red interna. Por ello, se recomienda fortalecer los controles de acceso, reducir la superficie de exposición y establecer políticas más estrictas de seguridad en los servicios desplegados.

Escaneo Nmap a la oficina de secretaría.

El escaneo ejecutado en los equipos de la oficina de secretaría permitió identificar configuraciones de red y servicios expuestos en el sistema operativo microsoft windows utilizados para la gestión de documentación institucional.

Los servicios detectados pueden permitir la enumeración de usuarios y el acceso no autorizado a recursos compartidos, la falta de políticas de control y monitoreo incrementa el riesgo de pérdida de integridad en la información administrativa.

Dominios COBIT relacionados:

- DSS02 – Gestión de incidentes y peticiones de servicio.
- EDM04 – Optimización del riesgo.

- APO12 – Gestión de riesgos.

Escaneo Nmap a la oficina de tecnologías de la información.

En la oficina de TI se realizó un escaneo técnico que estuvo orientado a identificar las vulnerabilidades en los equipos que están encargados del soporte y la administración de los sistemas de reclutamiento y como resultado se evidenció, la presencia de servicios abiertos y herramientas remotas que requieren el control y supervisión constante, todo esto debido a su potencial impacto en la seguridad operativa.

- Puertos abiertos detectados: 135 (Microsoft RPC), 139 (NetBIOS-SSN), 445 (Microsoft-DS), 5357 (HTTP Microsoft HTTPAPI 2.0) y 7070 (AnyDesk SSL).
- Sistema operativo identificado: Microsoft Windows 10.
- Servicio remoto detectado: AnyDesk Client con certificado SSL activo y sin restricción de autenticación.

El análisis evidencia vulnerabilidades derivadas del uso de servicios SMB y NetBIOS abiertos, además de herramientas de acceso remoto sin mecanismos de registro ni auditoría, estas condiciones exponen al entorno tecnológico a accesos no controlados y comprometen la disponibilidad y seguridad de la información institucional.

Dominios COBIT relacionados:

- APO10 – Gestión de proveedores.
- DSS05 – Gestión de la seguridad de los servicios.
- MEA02 – Supervisión, evaluación y valoración del sistema de control interno.

Los resultados obtenidos demuestran que la red institucional del GIR necesita fortalecerse urgentemente requerimos implementar controles de seguridad perimetral más sólidos, una segmentación de red adecuada, auditorías regulares de servicios y políticas de autenticación robustas estas acciones deben alinearse con las prácticas establecidas en el marco COBIT 2019. Solo así garantizaremos una gestión efectiva de la información y reduciremos consistentemente los riesgos tecnológicos que enfrenta la organización.

Analisis de vulnerabilidades NMAP

Con el propósito de analizar los hallazgos obtenidos a partir de los escaneos de red realizados en los tres departamentos evaluados (Talento humano, secretaría y TI), se elaboró una matriz comparativa en la que se detallan las vulnerabilidades identificadas, el riesgo que representan y la correspondencia con los dominios y subdominios de COBIT 2019 que se han considerado en este estudio. La Tabla XI sintetiza esta información, permitiendo visualizar de manera integral cómo cada hallazgo técnico puede ser gestionado mediante las buenas prácticas establecidas en el marco de referencia Cobit 2019.

Tabla XI.
VULNERABILIDADES DETECTADAS POR DEPARTAMENTO Y RELACIÓN CON DOMINIOS COBIT 2019

Departamento.	**Vulnerabilidad.**	**Subdominio relacionado.**
Talento Humano.	Exposición de puertos 135, 139 y 445 abiertos.	EDM04 – Asegurar la optimización del riesgo; DSS05 – Gestión de la seguridad de los servicios.
Talento Humano.	Uso de AnyDesk sin controles de seguridad robustos.	APO12 – Gestión de riesgos; DSS05 – Gestión de la seguridad de los servicios.
Secretaría.	Puerto 445/tcp (SMB) sin firma obligatoria.	DSS05 – Gestión de la seguridad de los servicios.
Secretaría.	Servicio HTTP habilitado (5357/tcp) sin utilidad clara.	APO12 – Gestión de riesgos.
Secretaría.	AnyDesk instalado con certificado de larga duración.	APO10 – Gestión de proveedores; DSS05 – Seguridad de los servicios.
TI.	Puertos 135/tcp (RPC), 139/tcp (NetBIOS) y 445/tcp (SMB) abiertos.	EDM04 – Optimización del riesgo; DSS05 – Seguridad de los servicios.

Continúa en la siguiente página

Continuación de la Tabla XI

Departamento.	**Vulnerabilidad.**	**Subdominio relacionado.**
TI.	Puerto 5357/tcp (HTTP) activo revelando información de servidor.	APO12 – Gestión de riesgos.
TI.	Configuraciones estándar de Windows sin hardening.	MEA01 – Supervisión del desempeño y conformidad; APO01 – Estrategia de TI.

El análisis de vulnerabilidades técnicas muestra una distribución irregular de hallazgos críticos en los diferentes departamentos de la organización como observamos en la Fig. 27, el departamento de TI acumula la mayor cantidad de incidencias reportadas esta concentración de riesgos evidencia la necesidad de reforzar los controles en el área tecnológica.

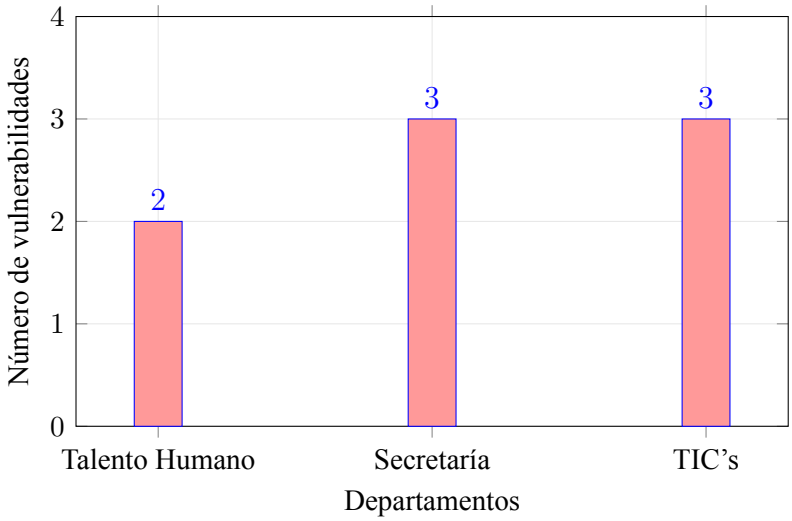

Fig. 27. Distribución de vulnerabilidades críticas detectadas por departamento.

La Tabla XII reúne los hallazgos de seguridad detectados. Cada vulnerabilidad técnica se vincula con sus dominios COBIT 2019 correspondientes para una gestión adecuada las direcciones IP evaluadas fueron 192.168.0.160 del área de Talento Humano, 192.168.8.255 de Secretaría y 192.168.8.69 del departamento de TIC's, esta correlación directa nos permite priorizar las acciones de mejora utilizando el marco de gobierno de TI como guía fundamental.

Tabla XII.

VULNERABILIDADES DETECTADAS EN SERVICIOS Y RELACIÓN CON DOMINIOS COBIT 2019

IP	**Puerto**	**Servicio**	**Estado**	**Riesgo**	**Dominio/Subdominio COBIT relacionado**
192.168.0.160	135,139,445	RPC, NetBIOS, SMB	Abiertos	Acceso remoto no autorizado.	EDM04, DSS05
192.168.0.160	AnyDesk	AnyDesk	Sin controles	Accesos remotos no autorizados.	APO12, DSS05
192.168.8.255	445/tcp	SMB	Sin firma	Ataques Man-in-the-Middle.	DSS05
192.168.8.255	5357/tcp	HTTP	Habilitado	Exposición innecesaria.	APO12
192.168.8.255	AnyDesk	AnyDesk	Certificado largo	Control remoto inseguro.	APO10, DSS05
192.168.8.69	135,139,445	RPC, NetBIOS, SMB	Abiertos	Explotación vulnerabilidades.	EDM04, DSS05
192.168.8.69	5357/tcp	HTTP	Activo	Filtración información.	APO12
192.168.8.69	Múltiples	Windows	Sin hardening	Configuraciones vulnerables.	MEA01, APO01

4.2 Etapa 2: Diagnóstico.

A partir de la encuesta a usuarios del sistema, la entrevista con el departamento de tecnologías y los escaneos técnicos realizados con NMAP, elaboramos un diagnóstico integral. Este análisis nos permitió determinar con precisión el estado actual del proceso de reclutamiento en cuanto a su gobernanza de TI, siempre bajo los parámetros establecidos por el marco COBIT 2019.

4.2.1 Resultados de identificación de brechas.

La encuesta a usuarios reveló percepciones divididas sobre el proceso de reclutamiento, si bien los entrevistados reconocieron un funcionamiento aceptable en ciertos aspectos operativos,

también expresaron inquietudes concretas sobre la protección de sus datos personales, además, mencionaron problemas relacionados con la disponibilidad del servicio y, de igual manera, señalaron la falta de canales claramente definidos para reportar incidentes, en conjunto, estos hallazgos indican que la experiencia del usuario final depende directamente de una implementación robusta de controles de seguridad así como de la continuidad operativa del servicio, por lo tanto, se evidencian áreas que requieren atención prioritaria para fortalecer la confianza y la eficiencia del proceso.

Por otro lado, en la entrevista que se realizó en el área de TI permitió identificar las fortalezas internas, como son la planificación de manera estratégica los recursos tecnológicos, también la existencia de capacitación en temas de seguridad informática y la definición de roles, entre las que destacaron la ausencia de mecanismos formales de cumplimiento normativo, la inexistencia de planes de respaldo documentados, las deficiencias en los controles de acceso a información sensible y la falta de auditorías periódicas que garantizaran la mejora continua.

El diagnóstico reveló que la organización presentó un nivel de madurez intermedio en la gobernanza de TI aplicada al proceso de reclutamiento, la Tabla XIII muestra que existieron prácticas en desarrollo y fortalezas puntuales, pero las debilidades detectadas constituyeron riesgos significativos para el cumplimiento de estándares de seguridad y normativas legales, este diagnóstico constituyó la base para la formulación de una propuesta de mejora alineada al marco Cobit 2019, orientada a fortalecer la protección de la información, garantizar la continuidad de los servicios y consolidar la confianza de los usuarios en el sistema de reclutamiento.

Tabla XIII.
COMPARACIÓN DE HALLAZGOS ENTRE ENCUESTA A USUARIOS Y ENTREVISTA AL ÁREA DE TI SEGÚN DOMINIOS COBIT 2019

Dominio / Sub-dominio.	**Aspecto.**	**Encuesta a usuarios.**	**Entrevista a TI.**
EDM03 / EDM04	Cumplimiento normativo.	No se perciben garantías de cumplimiento de normativas.	Falta de mecanismos formales de supervisión y auditorías previas.

Continúa en la siguiente página

Continuación de la Tabla XIII

Dominio / Sub-dominio.	**Aspecto.**	**Encuesta a usuarios.**	**Entrevista a TI.**
APO12	Gestión de riesgos.	Usuarios poco informados sobre medidas preventivas.	Se reporta capacitación y acciones preventivas implementadas.
APO10	Gestión de proveedores.	No se identifican criterios claros de control en encuestas.	Roles y responsabilidades definidos en la gestión de proveedores.
BAI03 / BAI07	Selección y pruebas de software.	Usuarios mencionan dificultades en plataformas de reclutamiento.	TI reconoce ausencia de criterios de selección formal, aunque sí realiza pruebas previas de aceptación.
DSS05	Seguridad de la información.	Preocupación por la protección de datos personales.	Reconocimiento de ausencia de controles efectivos de acceso.
DSS04	Continuidad del servicio.	Inquietud por fallas y falta de respaldo en el sistema.	No existen planes documentados de recuperación y respaldo.
DSS02	Atención de incidentes.	Dificultades en comunicación y seguimiento de casos.	Respuesta oportuna y registro de incidentes con soporte técnico.
MEA02	Auditorías.	Usuarios no perciben mecanismos de control externo.	Falta de auditorías internas o externas periódicas.

Riesgos detectados con pruebas técnicas (Nmap).

Durante la etapa de diagnóstico identificamos y clasificamos los riesgos en los sistemas informáticos de tres áreas clave como talento humano, secretaría y la oficina de TI, los hallazgos

obtenidos mediante el escaneo técnico nos permiten organizar estos riesgos en dos categorías principales.

- **Acceso no autorizado:** Encontramos puertos y servicios expuestos sin la protección necesaria, lo que, en consecuencia, facilita intrusiones tanto externas como internas, además, este fallo de seguridad se conecta directamente con tres dominios del marco COBIT: DSS05, por la falta de controles de acceso diferenciados; APO12, debido a la ausencia de medidas proactivas para prevenir ataques; y MEA01, por el monitoreo insuficiente de incidentes de seguridad, de este modo, la evidencia revela que las debilidades técnicas identificadas tienen un impacto transversal en los procesos de gestión, defensa y supervisión de TI.

- **Pérdida de datos:** La falta de mecanismos de respaldo confiables y protocolos de recuperación validados nos expone ante fallos técnicos o ciberataques este riesgo impacta DSS04 al carecer de planes de recuperación ante desastres afecta BAI07 por la documentación insuficiente en herramientas de respaldo y compromete EDM04 con una gestión deficiente de riesgos en procesos críticos.

Mediante la clasificación de riesgos se pudo obtener el un punto de partida para la priorización de acciones de mejora, que van a estar orientadas en robustecer los sistemas de seguridad de la información en el departamento de talento humano del GIR, bajo el marco Cobit 2019.

4.2.2 Resultados de matriz de riesgos.

En la Tabla XIV se presenta la matriz de riesgos construida a partir de los resultados obtenidos en la encuesta a usuarios y la entrevista al área de TI, en ella se identifican los riesgos principales asociados al proceso de reclutamiento, sus causas, nivel de probabilidad e impacto, así como las acciones de mitigación propuestas en concordancia con los lineamientos del marco Cobit 2019, esta herramienta permitió priorizar los riesgos críticos relacionados con la seguridad de la información, la continuidad del servicio y el cumplimiento normativo, aspectos que resultan fundamentales para garantizar la confianza y la transparencia en los procesos institucionales.

Tabla XIV.

MATRIZ DE RIESGOS DEL PROCESO DE RECLUTAMIENTO SEGÚN COBIT 2019

Dominio / Subdominio	**Riesgo identificado**	**Causa principal**	**Prob.**	**Impacto**	**Acción de mitigación propuesta**
EDM03 / EDM04	Incumplimiento de normativas de protección de datos.	Falta de políticas y supervisión formal.	Alta.	Alto.	Establecer políticas documentadas y auditorías de cumplimiento.
APO12	Brechas en la gestión de riesgos de TI.	Usuarios poco informados y capacitación limitada.	Media.	Alto.	Programas de capacitación continua y planes de concientización.
BAI03	Selección inadecuada de software de reclutamiento.	Ausencia de criterios de evaluación y documentación.	Media.	Medio.	Definir lineamientos de selección basados en seguridad y compatibilidad.
DSS05	Acceso no autorizado a información sensible de aspirantes.	Falta de controles efectivos de seguridad.	Alta.	Alto.	Implementar control de accesos basado en roles y monitoreo de actividad.
DSS04	Pérdida de datos de candidatos por falta de respaldos.	Inexistencia de políticas de respaldo y recuperación.	Media.	Alto.	Implementar respaldos automatizados y pruebas de recuperación periódicas.
DSS02	Retrasos en la atención de incidentes.	Deficiencias en comunicación y seguimiento.	Media.	Medio.	Establecer procedimientos estandarizados y SLA claros.

Continúa en la siguiente página

Continuación de la Tabla XIV

Dominio / Subdominio	Riesgo identificado	Causa principal	Prob.	Impacto	Acción de mitigación propuesta
MEA02	Falta de auditorías periódicas.	Inexistencia de procesos de evaluación formal.	Media.	Alto.	Programar auditorías internas y externas de forma anual.
MEA03	Ineficacia en la evaluación de medidas de mitigación.	Acciones correctivas no documentadas ni medidas con indicadores.	Media.	Medio.	Establecer métricas de control y documentación formal de medidas.

La Fig. 28 muestra el mapa de calor de los riesgos identificados en el proceso de reclutamiento, elaborado en función de la probabilidad de ocurrencia y el impacto que tendrían en la organización, se observa que los riesgos más críticos corresponden a la seguridad de la información (DSS05) y la continuidad del servicio (DSS04), ambos ubicados en la zona de alta probabilidad y alto impacto, asimismo, riesgos como el cumplimiento normativo (EDM03/04) y la falta de auditorías (MEA02) se ubican en áreas de atención prioritaria, mientras que la gestión de riesgos (APO12) y la atención de incidentes (DSS02) se consideran de menor impacto relativo.

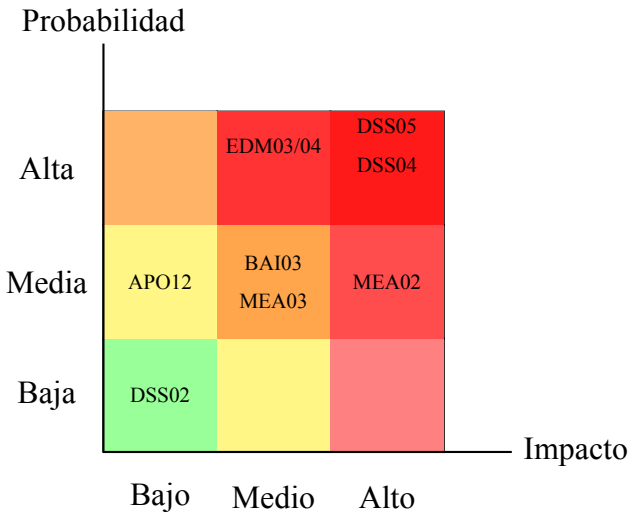

Fig. 28. Mapa de calor de riesgos del proceso de reclutamiento en función de probabilidad e impacto

Controles Existentes.

Durante el diagnóstico se realizó la revisión de los controles técnicos y administrativos implementados en el departamento de talento humano, la oficina de secretaría y la oficina de TI, el análisis nos permitió evidenciar tanto prácticas que contribuyen a la protección de la información como debilidades que exponen a la organización a riesgos significativos.

Documentar Controles.

- La mayoría de equipos operan con Windows actualizado, lo que asegura parches de seguridad recientes. El protocolo SMB tiene firma digital configurada aunque no es obligatoria. Contamos con AnyDesk autorizado para soporte técnico y continuidad operativa. El acceso a sistemas institucionales se maneja con contraseñas establecidas, mientras algunos departamentos realizan respaldos manuales de forma reactiva cuando lo consideran necesario.

Debilidades detectadas.

- La firma digital en SMB sigue siendo opcional, una condición que abre la puerta a ataques de tipo Man-in-the-Middle, servicios sensibles como RPC, NetBIOS y SMB permanecen expuestos sin una segmentación adecuada ni restricciones de acceso definidas el software de acceso remoto AnyDesk opera sin autenticación multifactor y carece de controles de auditoría suficientes, no existen procedimientos documentados para respaldar y recuperar datos, tampoco se realizan pruebas periódicas que validen estos procesos. Las políticas institucionales sobre el uso de tecnología en reclutamiento resultan ambiguas o inexistentes la formación del personal en gestión de riesgos y seguridad informática presenta deficiencias importantes el monitoreo de indicadores de seguridad, desempeño y cumplimiento normativo se lleva a cabo de manera limitada.

La evaluación refleja que aunque existen ciertos controles básicos en los departamentos analizados, estos resultan insuficientes para garantizar la protección de la información crítica y el cumplimiento normativo, las debilidades identificadas justifican la necesidad de diseñar e implementar un plan de mejoras bajo el marco de Cobit 2019, con énfasis en los dominios de gestión de riesgos (APO12), seguridad de los servicios (DSS05) y continuidad del servicio (DSS04).

4.2.3 Resultados de cumplimiento normativo Cobit 2019.

La Tabla XV presenta el cumplimiento normativo del proceso de reclutamiento según los dominios y subdominios de Cobit 2019, los resultados obtenidos de la entrevista al área de TI y de la encuesta a usuarios reflejan que, si bien existen fortalezas en la planificación estratégica, gestión de riesgos y proveedores, persisten debilidades críticas en el cumplimiento normativo, la continuidad del servicio, la seguridad de la información y las auditorías, asimismo, se identificó un control parcialmente implementado en la evaluación de medidas de mitigación de riesgos (MEA03), estos hallazgos evidencian la necesidad de un plan de mejora que formalice políticas, implemente auditorías periódicas y fortalezca la transparencia frente a los usuarios.

Tabla XV.
CUMPLIMIENTO NORMATIVO SEGÚN COBIT 2019 EN TODOS LOS DOMINIOS EVALUADOS

Dominio / Subdominio.	**Evidencia (Entrevista TI).**	**Percepción (Encuesta usuarios).**	**Estado de cumplimiento.**
EDM01 – Alineación de TI con la estrategia	Se reporta alineación parcial con los objetivos institucionales.	Usuarios perciben que TI apoya procesos pero no existe claridad normativa.	✓ Cumple.
EDM03 – Cumplimiento con requerimientos externos.	No existen mecanismos formales de supervisión de normativas.	No perciben garantías de cumplimiento en protección de datos.	✗ No cumple.
EDM04 – Optimización del riesgo.	No se evidencian políticas documentadas sobre riesgos regulatorios.	Se percibe desconfianza en la transparencia del proceso.	✗ No cumple.
APO01 – Gestión de la estrategia de TI.	Evidencia de planificación estratégica y recursos documentados.	Usuarios valoran disponibilidad tecnológica para procesos.	✓ Cumple.
APO10 – Gestión de proveedores.	Roles y responsabilidades definidos en contratos.	Usuarios perciben continuidad adecuada en servicios externos.	✓ Cumple.

Continúa en la siguiente página

Continuación de la Tabla XV

Dominio / Subdominio.	**Evidencia (Entrevista TI).**	**Percepción (Encuesta usuarios).**	**Estado de cumplimiento.**
APO12 – Gestión de riesgos.	Se realizan capacitaciones y acciones preventivas.	Usuarios poco informados sobre medidas de prevención.	✓ Cumple.
BAI03 – Selección de software.	Ausencia de criterios formales de evaluación de software.	Usuarios perciben deficiencias en plataformas de reclutamiento.	✗ No cumple.
BAI06 – Gestión de cambios.	Se evalúa la seguridad antes de implementar cambios.	Usuarios perciben mejoras progresivas en sistemas.	✓ Cumple.
BAI07 – Pruebas de aceptación y transición.	Se realizan pruebas de aceptación documentadas.	Usuarios perciben estabilidad en nuevas herramientas.	✓ Cumple.
DSS05 – Seguridad de la información.	No existen controles efectivos de acceso a datos sensibles.	Usuarios preocupados por la confidencialidad de la información personal.	✗ No cumple.
DSS04 – Continuidad del servicio.	No existen planes documentados de respaldo y recuperación.	Usuarios reportan fallas y ausencia de mecanismos de respaldo.	✗ No cumple.
DSS02 – Gestión de incidentes.	Se responde de manera oportuna a incidentes registrados.	Usuarios perciben demoras y falta de seguimiento a casos.	✓ Cumple.
MEA01 – Indicadores de desempeño.	Se miden indicadores de TI y seguridad.	Usuarios no tienen acceso a los indicadores, pero perciben estabilidad.	✓ Cumple.

Continúa en la siguiente página

Continuación de la Tabla XV

Dominio / Subdominio.	**Evidencia (Entrevista TI).**	**Percepción (Encuesta usuarios).**	**Estado de cumplimiento.**
MEA02 – Auditorías internas y externas.	No existen auditorías periódicas de cumplimiento.	Usuarios consideran que no hay control externo ni transparencia.	✗ No cumple.
MEA03 – Medidas de mitigación de riesgos.	Acciones correctivas informales, sin indicadores.	Usuarios perciben debilidad en seguimiento y control.	∂ Parcial.

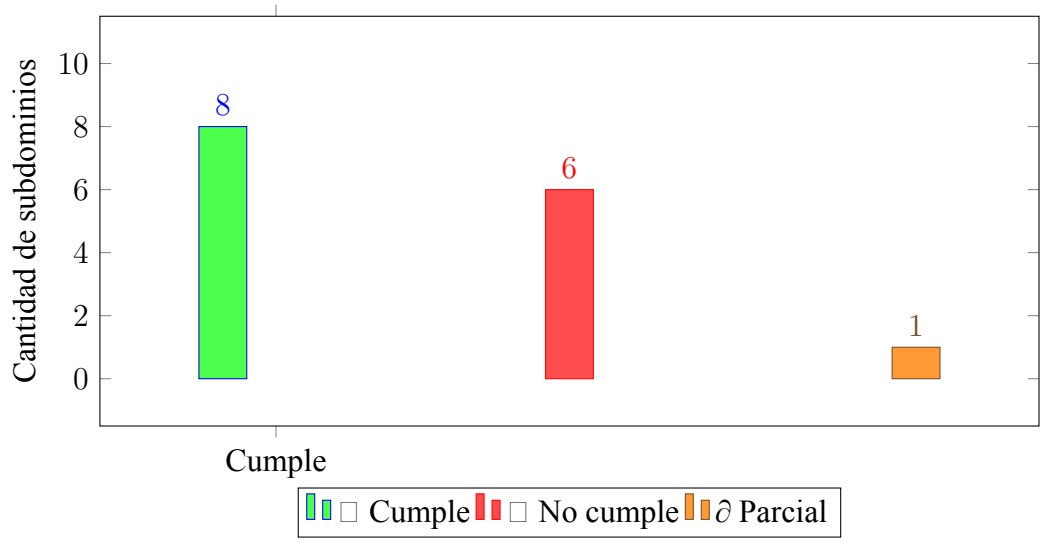

Fig. 29. Distribución del cumplimiento normativo en los subdominios COBIT 2019 evaluados

Tal como se aprecia en la Fig. 29, de los 15 subdominios Cobit 2019 evaluados en el proceso de reclutamiento, 8 (53 %) cumplen con los estándares establecidos, 6 (40 %) no cumplen y 1 (7 %) presenta un cumplimiento parcial, estos resultados reflejan una implementación desigual, donde si bien más de la mitad de los controles son adecuados, existen áreas críticas que requieren atención inmediata, particularmente en cumplimiento normativo, seguridad de la información y auditorías.

4.3 Etapa 3: Evaluación.

Una vez recopilada y analizada la información proveniente de las encuestas aplicadas a los usuarios y de la entrevista realizada al área de tecnologías de la información, se procedió a la

fase de evaluación, en esta etapa se contrastaron los resultados obtenidos con los lineamientos establecidos en el marco de referencia Cobit 2019, a fin de determinar el nivel de cumplimiento de los controles asociados al proceso de reclutamiento.

Esta evaluación buscó determinar con exactitud el nivel de cumplimiento de la organización frente a los dominios y procesos de COBIT 2019, identificando sus fortalezas, debilidades y aquellos aspectos con implementación parcial, el diagnóstico obtenido servirá como base para construir una propuesta de mejora que garantice la seguridad, el cumplimiento normativo y la eficiencia dentro del proceso de reclutamiento.

4.3.1 Resultados de indicadores CIA: Confidencialidad - Integridad - Disponibilidad.

En la evaluación se aplicaron los indicadores CIA (Confidencialidad, Integridad y Disponibilidad) como criterios transversales a los dominios de Cobit 2019 utilizados en el análisis, estos indicadores permiten medir de manera objetiva cómo se gestionan los aspectos críticos de seguridad de la información en el proceso de reclutamiento:

- **Confidencialidad:** Protección de los datos personales de los aspirantes y control de accesos a la información sensible.
- **Integridad:** Nos ayuda asegurar de que la información se mantiene exacta, completa y libre de modificaciones no autorizadas.
- **Disponibilidad:** Mantenimiento de la continuidad operativa de las plataformas de captación de talento, minimizando el tiempo de inactividad y garantizando la accesibilidad mediante infraestructuras con tolerancia a fallos.

La Tabla XVI presenta la aplicación de los indicadores CIA a los dominios COBIT 2019 estudiados. En primer lugar, el dominio APO muestra el mayor nivel de cumplimiento; mientras tanto, EDM y DSS presentan debilidades importantes en los tres indicadores, por su parte, BAI refleja un nivel intermedio, aunque con fallas específicas en integridad, y MEA mantiene controles parciales sobre disponibilidad y cumplimiento normativo, en conjunto, estos hallazgos confirman la urgencia de reforzar las políticas de confidencialidad, garantizar la integridad

mediante auditorías regulares e implementar planes de continuidad que aseguren la disponibilidad de los servicios críticos para el proceso de reclutamiento, además, esta evidencia permite orientar las acciones prioritarias en materia de gobernanza y seguridad de la información.

Tabla XVI.
INDICADORES CIA APLICADOS A LOS DOMINIOS COBIT 2019 EVALUADOS

Dominio	**Confidencialidad**	**Integridad**	**Disponibilidad**
EDM (Evaluar, Dirigir y Monitorear).	Falta de mecanismos normativos claros para proteger datos personales (✗).	Inexistencia de auditorías que validen exactitud de registros (✗).	Gestión de riesgos sin planes documentados (✗).
APO (Alinear, Planear y Organizar).	Definición de roles y control en proveedores (✓).	Estrategia y planificación aseguran consistencia de información (✓).	Capacitación en riesgos fortalece continuidad (✓).
BAI (Construir, Adquirir e Implementar).	Seguridad revisada en cambios y pruebas (✓).	Ausencia de criterios documentados para selección de software (✗).	Pruebas garantizan estabilidad de nuevas herramientas (✓).
DSS (Entregar, Dar servicio y Soportar).	Accesos a información sensible sin controles efectivos (✗).	Gestión de incidentes mantiene registros consistentes (✓).	Falta de planes de respaldo y recuperación (✗).
MEA (Monitorear, Evaluar y Valorar).	Cumplimiento regulatorio percibido como débil (✗).	Indicadores de desempeño parcialmente medidos (✓).	Medidas de mitigación aplicadas de forma parcial (∂).

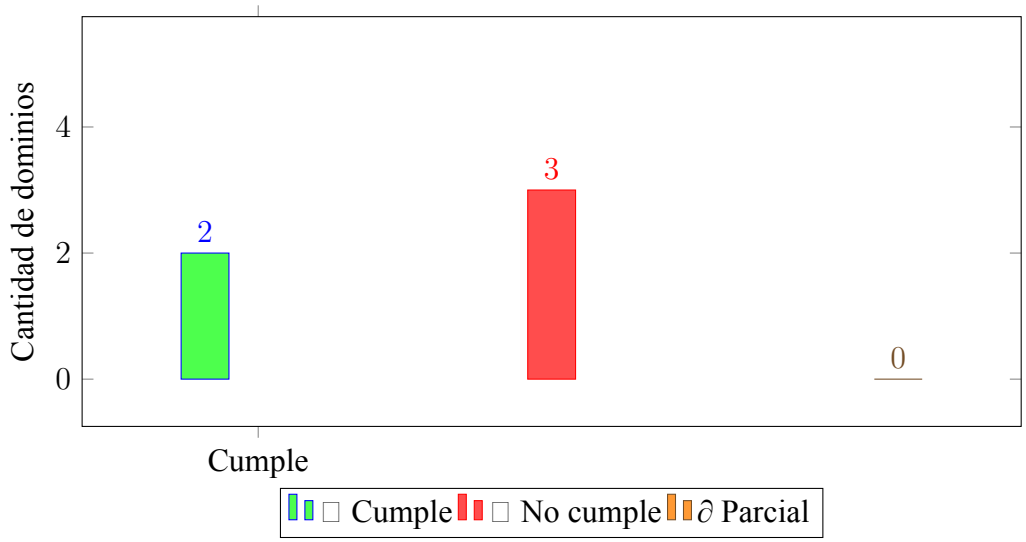

Fig. 30. Nivel de cumplimiento en Confidencialidad por dominio COBIT 2019

En la Fig. 30 se observa que de los 5 dominios evaluados, solo 2 (40 %) cumplen con los requisitos de confidencialidad, mientras que 3 (60 %) presentan deficiencias. Los dominios APO y BAI demuestran controles adecuados, mientras que EDM, DSS y MEA requieren mejoras urgentes en la protección de datos sensibles.

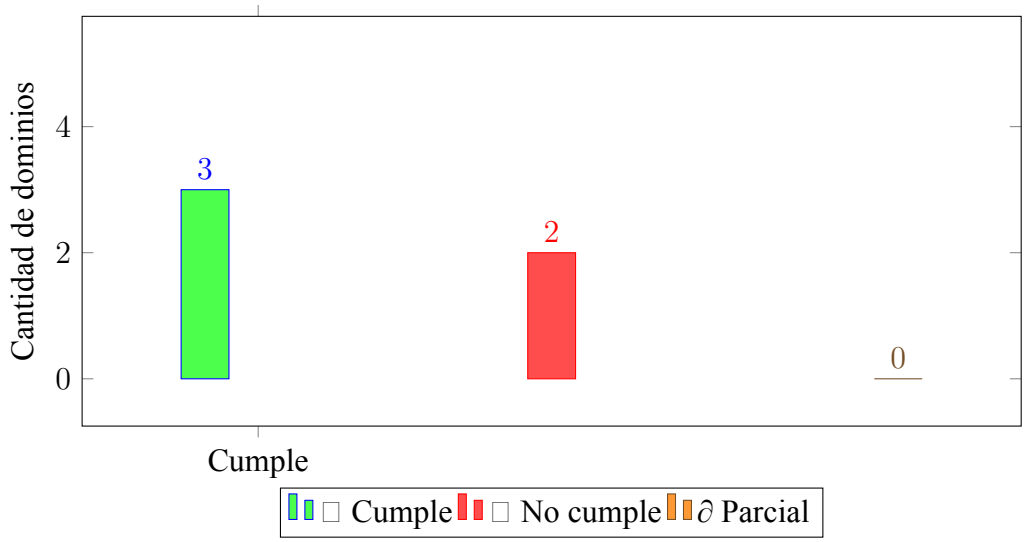

Fig. 31. Nivel de cumplimiento en Integridad por dominio COBIT 2019

Como se muestra en la Fig. 31, 3 de los 5 dominios (60 %) cumplen con los estándares de integridad, destacándose APO, DSS y MEA. Sin embargo, EDM y BAI presentan vulnerabilidades que afectan la exactitud y consistencia de la información, requiriendo atención en criterios de selección de software y auditorías.

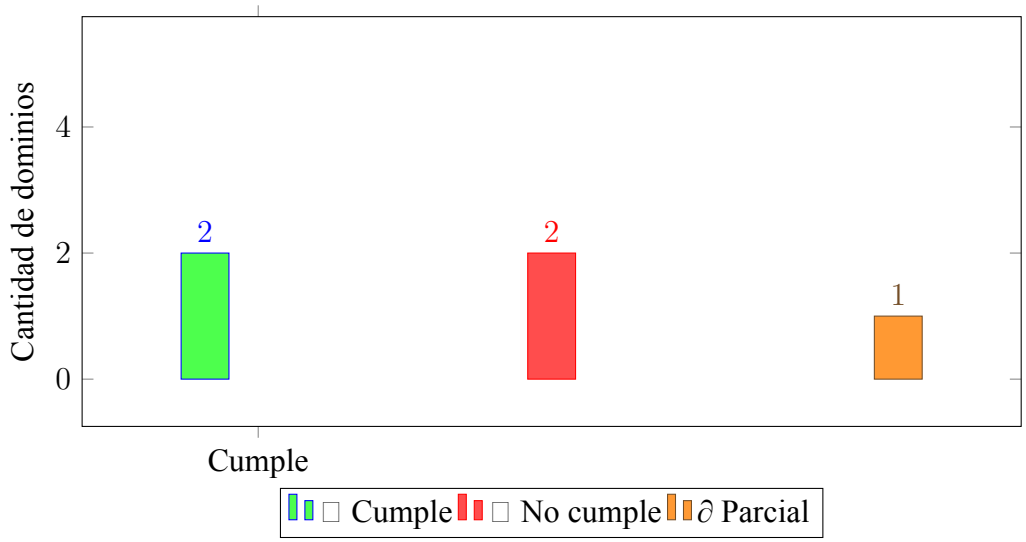

Fig. 32. Nivel de cumplimiento en Disponibilidad por dominio COBIT 2019

En la Fig. 32 nos muestra que en disponibilidad solo 2 dominios cumplen a plenitud, otros 2 no alcanzan el nivel requerido y 1 mantiene un cumplimiento parcial. APO y BAI garantizan la continuidad operativa, EDM y DSS carecen de planes de respaldo, mientras MEA necesita reforzar sustancialmente sus medidas de mitigación.

4.3.2 Aplicación de Cobit 2019.

La aplicación del marco de referencia Cobit 2019 permitió evaluar de manera estructurada el proceso de reclutamiento en la organización, considerando los dominios y subdominios seleccionados a partir de las encuestas aplicadas a los usuarios y la entrevista realizada al departamento de tecnologías de la información, a continuación se detallan los principales resultados de cada dominio:

EDM – Evaluar, Dirigir y Monitorear.

- **EDM01 – Asegurar la alineación de TI con la estrategia:** Pudimos ver que existían políticas institucionales generales; sin embargo, no se encontraron lineamientos específicos que integren de manera formal la estrategia de TI con los procesos de reclutamiento.
- **EDM03 – Asegurar cumplimiento con requerimientos externos:** Se pudo detectar que el área de TI, no contaba con mecanismos lo suficientes adecuado en seguimiento y documentación frente a las normativas de protección de datos personales, esto representa una debilidad relevante en materia de cumplimiento normativo.

- **EDM04 – Asegurar la optimización del riesgo:** Identificamos la existencia de prácticas aisladas de control; no obstante, estas no se enmarcan dentro de un esquema formal de monitoreo y gestión de riesgos relacionados con el uso de TI en el área de talento humano.

APO – Alinear, Planear y Organizar.

- **APO01 – Gestión de la estrategia de TI:** para apoyar los procesos institucionales, se ha confirmado que la institución esta en constante actualización, esto incluye también el proceso de reclutamiento, los planes estratégicos son documentados y se respaldan esta gestión y, a su vez, permiten una alineación coherente entre los objetivos organizacionales y las capacidades tecnológicas disponibles.
- **APO10 – Gestión de proveedores:** Se pudo Verificar claramente la existencia de contratos vigentes y roles definidos que yudan en la administración del software de reclutamiento, esto es lo que garantiza la supervisiób adecuada de los servicios externos y así mismo, esta estructura logra contribuir a mantener la continuidad operativa y a fortalecer la rendición de cuentas por parte de los proveedores.
- **APO12 – Gestión de riesgos:** se pudo verificar que i exiten capacitaciones constantes al personal esto ayuda a identificar y mitigar riesgos informáticos, donde se fortalece de manera progresiva una cultura institucional de seguridad y así del mismo modo, estas acciones preventivas permiten anticipar posibles incidentes y mejorar la resiliencia tecnológica del proceso de reclutamiento.

BAI – Construir, Adquirir e Implementar.

- **BAI03 – Gestión de soluciones identificadas y construidas:** Los procesos de aprovisionamiento y mantenimiento evolutivo del software de reclutamiento operaban sin métricas de selección estandarizadas; esta ausencia de protocolos de validación derivó en una gestión de activos de software carente de una arquitectura de referencia técnica.
- **BAI06 – Gestión de cambios:** Cada modificación en los sistemas pasaba por una revisión de seguridad antes de su aprobación y, además, contaba con validaciones técnicas previas. De este modo, se consolidaba el proceso formal de gestión de cambios y se reducía el riesgo de introducir vulnerabilidades en el entorno operativo.

- **BAI07 – Aceptación y transición de cambios:** Todas las nuevas herramientas o actualizaciones requerían pruebas de aceptación antes de su implementación en producción, asegurando así una transición controlada y minimizando fallos derivados de configuraciones incorrectas o incompatibilidades.

DSS – Entregar, Dar Servicio y Soportar.

- **DSS05 – Gestión de la seguridad de los servicios:** La arquitectura de control de accesos sobre los activos de información de los candidatos exhibe vulnerabilidades estructurales; esta ausencia de privilegios mínimos y segregación de perfiles de usuario exacerba la probabilidad de exfiltración de datos. La carencia de mecanismos de autenticación granular incrementa drásticamente el vector de riesgo para la confidencialidad sistémica.
- **DSS04 – Continuidad del servicio:** No se encontraron procedimientos formalizados de respaldo y recuperación; en consecuencia, se evidencia una vulnerabilidad importante frente a la disponibilidad del servicio, esta ausencia de mecanismos de contingencia compromete la respuesta institucional ante fallos inesperados.
- **DSS02 – Gestión de incidentes y peticiones de servicio:** Se verificó que los incidentes eran atendidos de forma oportuna por el área técnica y que, en general, se mantenían tiempos de respuesta aceptables, no obstante, se observó la necesidad de fortalecer la sistematización del registro y análisis de incidentes para mejorar la retroalimentación operativa.

MEA – Monitorear, Evaluar y Valorar.

- **MEA01 – Supervisión del desempeño y la conformidad:** La organización realiza un seguimiento de indicadores básicos de desempeño; sin embargo, estos no se alinean completamente con los estándares de seguridad establecidos, además, se evidencian limitaciones en el uso de datos para la toma de decisiones.
- **MEA02 – Supervisión del control interno:** La intermitencia en los ciclos de auditoría interna erosiona la capacidad de telemetría sobre la eficacia de los controles; tal discontinuidad técnica impide la remediación oportuna de desviaciones operativas, lo que hace imperativa la institucionalización de un cronograma de fiscalización que garantice la trazabilidad del cumplimiento.

- **MEA03 – Supervisión del cumplimiento externo:** La validación de las salvaguardas frente a amenazas se ejecuta bajo un enfoque fragmentado y carente de pruebas de estrés que certifiquen su resiliencia; consecuentemente, la falta de una verificación empírica de los controles perpetúa brechas de seguridad que obstaculizan la madurez de un ecosistema de gobernanza robusto.

La aplicación del marco Cobit 2019 permitió identificar fortalezas en la planificación estratégica, la gestión de proveedores y la capacitación en riesgos (APO01, APO10 y APO12), así como en la gestión de cambios y las pruebas de aceptación (BAI06 y BAI07). Sin embargo, también se evidenciaron debilidades en cumplimiento normativo, continuidad del servicio, seguridad de la información y auditorías (EDM03, DSS04, DSS05 y MEA02), además de controles aplicados de manera parcial (MEA03), como se detalla en la Tabla XVII.

Tabla XVII.
RESUMEN COMPARATIVO DE CUMPLIMIENTO DE DOMINIOS COBIT 2019 EN EL PROCESO DE RECLUTAMIENTO

Dominio / Subdominio	**Descripción**	**Cumplimiento**
EDM01	Asegurar la alineación de TI con la estrategia.	✓
EDM03	Cumplimiento con requerimientos externos.	✗
EDM04	Optimización del riesgo.	✗
APO01	Gestión de la estrategia de TI.	✓
APO10	Gestión de proveedores.	✓
APO12	Gestión de riesgos.	✓
BAI03	Selección y actualización del software de reclutamiento.	✗
BAI06	Evaluación de seguridad en cambios.	✓
BAI07	Pruebas de aceptación y transición.	✓
DSS05	Seguridad de la información de aspirantes.	✗
DSS04	Continuidad del servicio.	✗

Continúa en la siguiente página

Continuación de la Tabla XVII

Dominio / Subdominio	Descripción	Cumplimiento
DSS02	Gestión de incidentes.	✓
MEA01	Medición de indicadores de desempeño y seguridad.	✓
MEA02	Auditorías internas y externas.	✗
MEA03	Evaluación de medidas de mitigación de riesgos.	∂

La Fig. 33 presenta el porcentaje de cumplimiento alcanzado por cada dominio de Cobit 2019 en el proceso de reclutamiento, se observa que el dominio APO alcanza un 100 % de cumplimiento, evidenciando una adecuada gestión estratégica y de riesgos, en contraste, los dominios EDM, DSS y MEA presentan un nivel de cumplimiento limitado (33.3 %), lo que refleja la necesidad de fortalecer los mecanismos de control, continuidad del servicio y cumplimiento normativo.

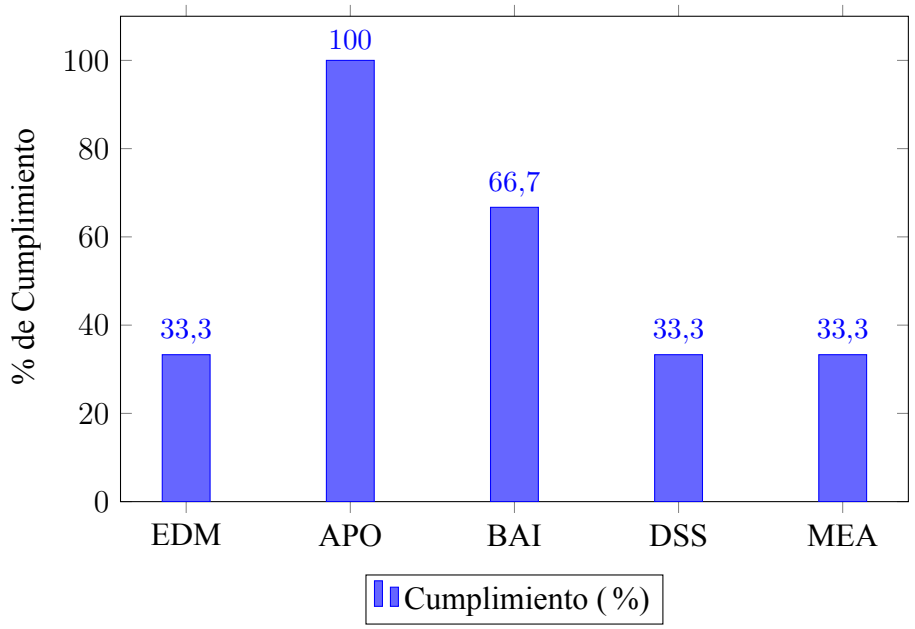

Fig. 33. Porcentaje de cumplimiento por dominio Cobit 2019.

4.4 Etapa 4: Propuesta de mejora.

4.4.1 Objetivo de propuesta de mejora.

La presente iniciativa articula el despliegue de salvaguardas técnicas y protocolos administrativos alineados al marco de gobernanza COBIT 2019, con el propósito de blindar los activos

de información en los procesos de captación del GIR. Se instituye un modelo de gobierno de TI resiliente orientado a la mitigación de vectores de riesgo; este esquema asegura el cumplimiento normativo mediante la formalización de políticas, el control de acceso bajo el principio de privilegios mínimos, la criptografía de datos en tránsito y una auditoría continua, optimizando la integridad en la gestión del capital humano.

4.4.2 Alcance de propuesta de mejora.

El alcance comprende el proceso completo de reclutamiento del GIR, incluyendo la postulación, selección y gestión de datos de aspirantes, abarca los sistemas tecnológicos involucrados, las políticas de seguridad de la información y los flujos de datos asociados, la intervención se aplica sobre cinco dominios, EDM (gobierno), APO (gestión), BAI (implementación), DSS (operación) y MEA (evaluación), incluye la formalización de políticas, controles de acceso, cifrado HTTPS, gestión de riesgos, continuidad del servicio y auditorías periódicas, beneficiando al departamento de talento humano y TI institucional.

4.4.3 Beneficiarios de la propuesta de mejora.

Los principales beneficiarios son el departamento de talento humano del GIR, que optimizará sus procesos de reclutamiento, los aspirantes, cuya información personal estará protegida y la institución policial en su conjunto, al fortalecer su seguridad informática, también se benefician el departamento de TI, con mejores prácticas de gobierno, y la ciudadanía ecuatoriana que contará con procesos más transparentes, la implementación impactará positivamente en la eficiencia operativa y la confiabilidad institucional del Grupo de Intervención y Rescate.

4.4.4 Mejoras propuestas según Cobit 2019.

La mitigación de las brechas de seguridad en el Departamento de Talento Humano del GIR se articula mediante un ecosistema de remediación bajo el estándar COBIT 2019, orientado a la formalización de la gobernanza corporativa de TI. En el eje estratégico, se instituye la normalización de directrices para el reclutamiento, garantizando que el aprovisionamiento tecnológico responda a una planificación sistemática basada en partidas presupuestarias y marcos temporales rigurosos. Respecto al robustecimiento técnico, la arquitectura propuesta adopta principios

de *Security by Design* y métricas OWASP para la validación de software, reforzando la confidencialidad de los aspirantes mediante la obligatoriedad de autenticación multifactor (2FA) y el cifrado de datos en tránsito vía HTTPS. La operatividad de este esquema descansa en la resiliencia proactiva, gestionada a través de un comité de control de cambios (CAB), simulacros de recuperación ante desastres (DRP) anuales y la transición hacia auditorías automatizadas continuas. Para asegurar la sostenibilidad del modelo, se prescribe la implementación de soluciones SIEM y ciclos de capacitación en ciberseguridad que utilicen ingeniería social simulada para consolidar una cultura de prevención institucional.

4.4.5 Evaluación Delphi a la propuesta de mejora.

El proceso de evaluación del plan de seguridad informática se desarrolló utilizando la metodología Delphi, con el fin de obtener consenso entre un panel de expertos en seguridad de la información, auditoría de TI y gestión de riesgos, este método es ampliamente utilizado en estudios donde se requiere la opinión de especialistas, permitiendo la convergencia progresiva hacia un acuerdo fundamentado mediante rondas sucesivas de evaluación.

El instrumento aplicado permitió evaluar 36 controles de seguridad basados en criterios de adecuación, pertinencia, nivel de implementación y capacidad de mitigación del riesgo, cada control fue valorado por siete expertos utilizando una escala Likert de 1 a 5.

La Tabla XVIII presenta los valores de media, mediana, moda, desviación estándar, rango intercuartílico y coeficiente de variación, de los 36 controles evaluados en la primera ronda Delphi, los resultados muestran una dispersión considerable entre evaluadores, especialmente en los controles 1, 3, 5, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33 y 35, evidenciando falta de consenso inicial.

Tabla XVIII.

ESTADÍSTICOS DESCRIPTIVOS DE LOS 36 CONTROLES EVALUADOS EN LA PRIMERA RONDA DELPHI

Control	Media	Mediana	Moda	DE	IQR	CV
1	2,571	3	4	1,272	2,0	0,495
2	4,429	5	5	0,787	1,0	0,178
3	3,000	3	3	1,000	0,5	0,333
4	4,143	5	5	1,069	2,0	0,258
5	3,429	4	4	1,272	1,0	0,371
6	4,286	5	5	0,951	1,5	0,222
7	3,714	4	5	1,113	1,5	0,300
8	4,000	4	4	0,816	1,0	0,204
9	3,714	4	4	1,380	1,0	0,372
10	4,143	4	5	0,900	1,5	0,217
11	3,571	4	4	1,272	0,5	0,356
12	4,286	5	5	0,951	1,5	0,222
13	3,714	4	4	1,380	1,0	0,372
14	4,143	4	5	0,900	1,5	0,217
15	3,571	4	4	1,272	0,5	0,356
16	4,286	5	5	0,951	1,5	0,222
17	3,714	4	4	1,380	1,0	0,372
18	4,143	4	5	0,900	1,5	0,217
19	3,571	4	4	1,272	0,5	0,356
20	4,143	4	5	0,900	1,5	0,217
21	3,714	4	4	1,380	1,0	0,372
22	4,286	5	5	0,951	1,5	0,222
23	3,714	4	4	1,380	1,0	0,372
24	4,143	4	5	0,900	1,5	0,217
25	3,429	4	4	1,272	1,0	0,371
26	4,286	5	5	0,951	1,5	0,222
27	3,429	4	4	1,272	1,0	0,371
28	4,143	4	5	0,900	1,5	0,217
29	3,714	4	4	1,380	1,0	0,372
30	4,143	4	5	0,900	1,5	0,217
31	3,714	4	4	1,380	1,0	0,372
32	4,286	5	5	0,951	1,5	0,222
33	3,286	3	3	1,254	1,0	0,382
34	4,286	5	5	0,951	1,5	0,222
35	3,429	4	4	1,272	1,0	0,371
36	4,143	4	5	0,900	1,5	0,217

Análisis gráfico y comparativo.

A continuación se presentan cuatro figuras basadas en los resultados estadísticos, medianas, desviación estándar, rango intercuartílico y coeficiente de variación, cada figura incluye una descripción y su interpretación dentro del contexto del método Delphi.

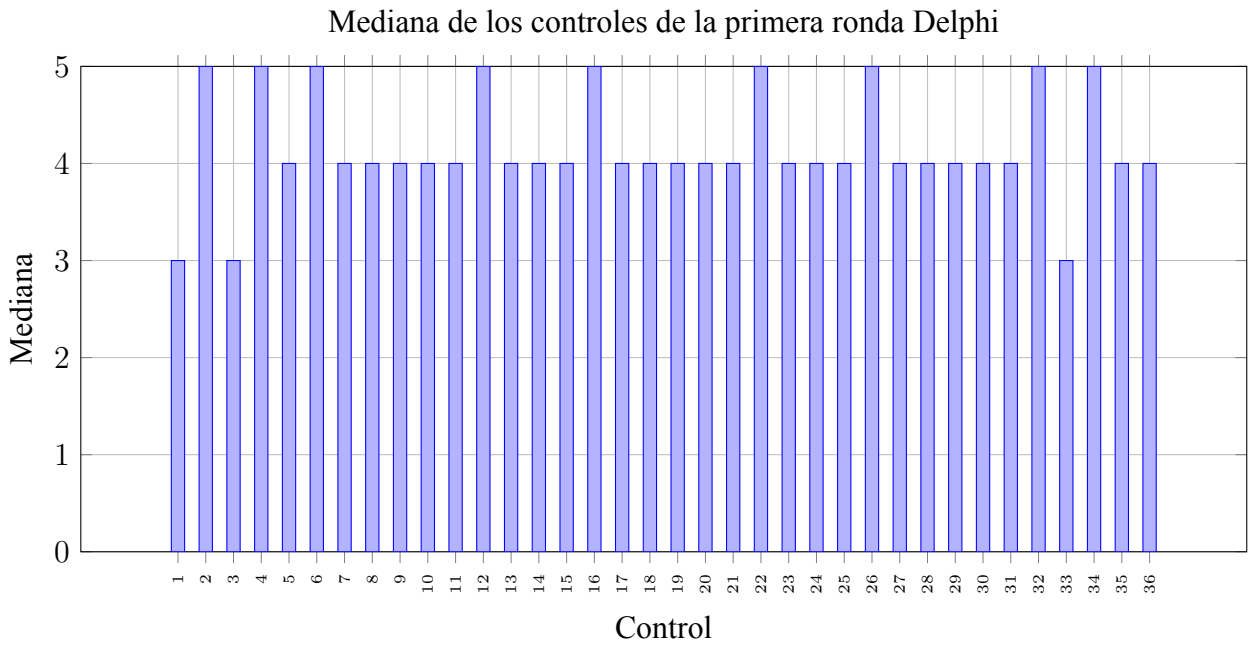

Fig. 34.
Mediana de cada control evaluado en la primera ronda Delphi.

Como vemos en la Figura 34 nos revela que la mayoría de controles registran medianas entre 3 y 4, mostrando una percepción generalizada de madurez intermedia entre los especialistas, los controles con mediana 3 señalan áreas de cumplimiento insuficiente que requieren atención inmediata, los controles con mediana 5 demuestran un amplio consenso respecto a su alto nivel de madurez alcanzado.

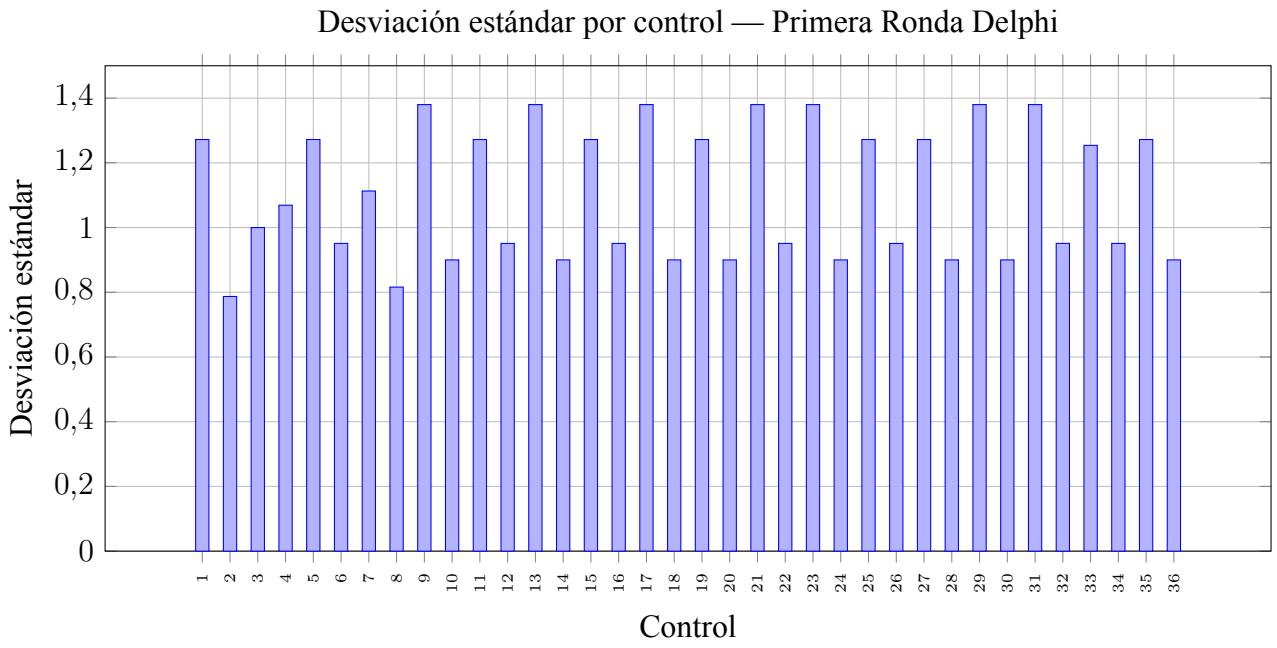

Fig. 35.
Variabilidad de las evaluaciones por control, medida mediante la desviación estándar.

La Figura 35 evidencia que algunos controles presentan alta dispersión, especialmente los controles 9, 13, 17, 21, 23, 29 y 31 con desviación estándar de 1.380, valores elevados de desviación estándar indican desacuerdo significativo entre los expertos, lo cual sugiere problemas de interpretación o implementación en dichos controles, los controles con menor dispersión (2, 8, 10, 14, 18, 20, 24, 28, 30, 36) muestran mayor consenso entre los evaluadores.

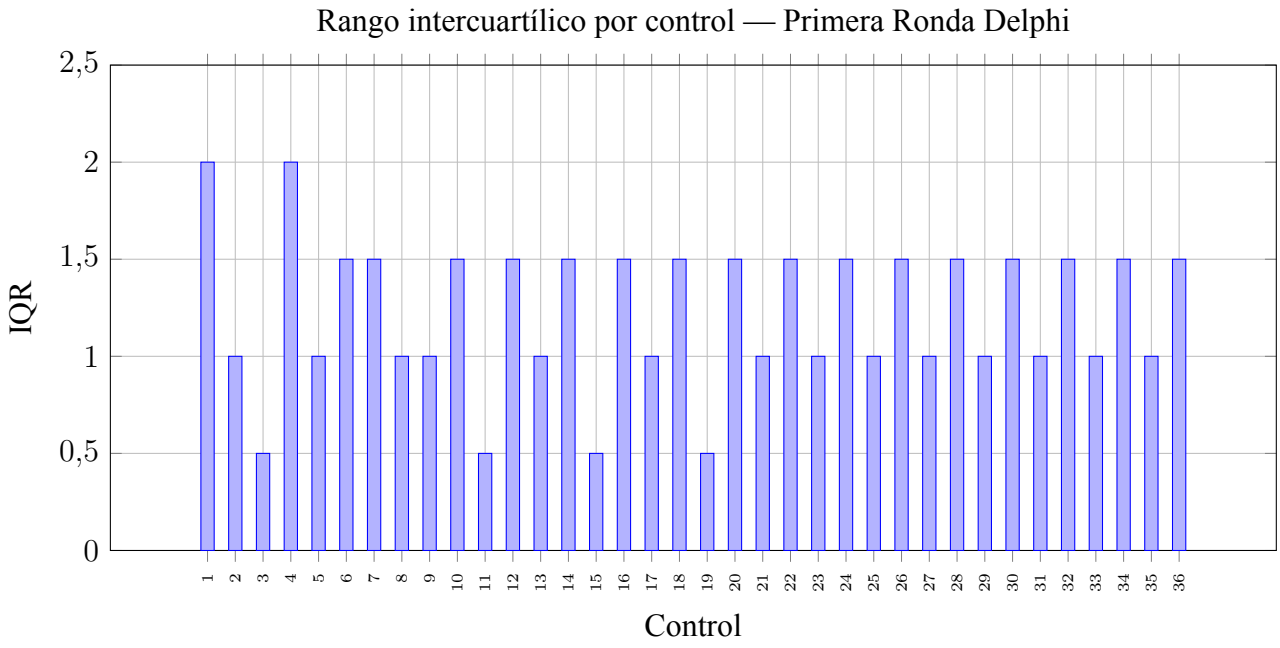

Fig. 36.
Rango intercuartílico (IQR) para cada control en la primera ronda Delphi.

Al examinar la Figura 36, se advierte que el ítem 1 exhibe el Rango Intercuartílico (IQR) más pronunciado (2,0), lo cual ratifica una heterogeneidad sustancial y la ausencia de una postura unificada en el panel. Una tendencia de dispersión idéntica se manifiesta en el control 4 ($IQR = 2{,}0$), denotando una volatilidad crítica en las métricas de evaluación asignadas; diametralmente, los controles 3, 11, 15 y 19 presentan una desviación mínima (0,5), fenómeno que consolida un grado de consenso robusto y una estabilización en el juicio de los especialistas para dichas variables.

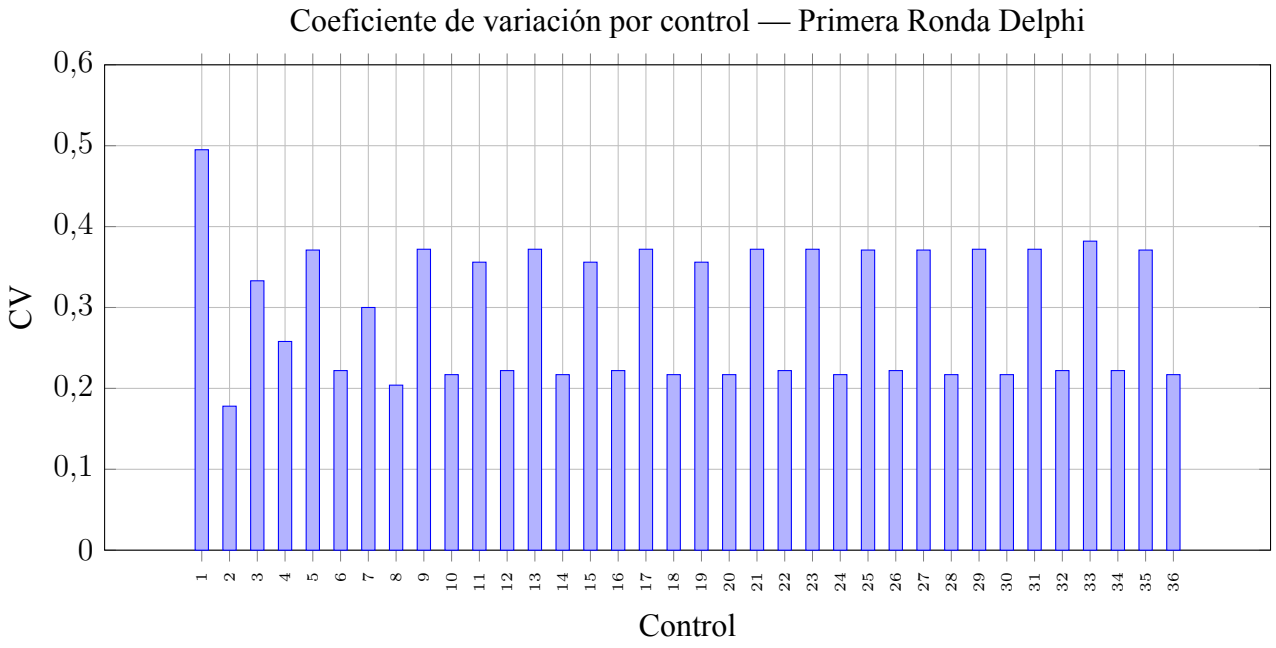

Fig. 37.
Coeficiente de variación de los 36 controles evaluados.

La Figura 37 sintetiza la variabilidad relativa, el control 1 presenta el valor más alto de coeficiente de variación (0.495), lo que indica que fue el más inestable en la evaluación de los expertos, los controles 9, 13, 17, 21, 23, 29 y 31 también muestran alta variabilidad relativa (CV = 0.372), controles con coeficiente de variación bajo (2, 10, 14, 18, 20, 24, 28, 30, 36 con CV ≈ 0.217-0.222) muestran mayor estabilidad y consenso entre los evaluadores.

4.4.6 Coeficiente de concordancia Kendall W

El coeficiente de concordancia de Kendall W se calcula para evaluar el grado de acuerdo entre múltiples evaluadores en estudios Delphi, la Ecuación 4 [50] del coeficiente W considerando la corrección por empates es:

$$W = \frac{12 \times S}{m^2 \times (n^3 - n) - m \times T} \tag{4}$$

Donde:

- W: Coeficiente de concordancia de Kendall (0 a 1)
- S: Suma de cuadrados de las desviaciones de los rangos totales
- m: Número de evaluadores (7 expertos)
- n: Número de ítems evaluados (36 controles)
- T: Corrección por empates entre los evaluadores
- 12: Constante de la fórmula

Sustituyendo con los valores calculados:

- $S = 58274{,}00$ (suma de cuadrados de las desviaciones)
- $T = 49,860$ (corrección total por empates)
- $m = 7$ expertos
- $n = 36$ controles

$$W = \frac{12 \times 58,274}{7^2 \times (36^3 - 36) - 7 \times 49,860} = \frac{699,288}{49 \times (46,656 - 36) - 349,020} = \frac{699,288}{49 \times 46,620 - 349,020}$$

$$W = \frac{699,288}{2,284,380 - 349,020} = \frac{699,288}{1,935,360} = 0{,}361$$

Prueba de significancia:

$$\chi^2 = m \times (n - 1) \times W = 7 \times (36 - 1) \times 0{,}361 = 7 \times 35 \times 0{,}361 = 88{,}445$$

El coeficiente de concordancia de Kendall W calculado para la primera ronda Delphi fue de $W = 0{,}361$ ($\chi^2 = 88{,}445$, $gl = 35$, $p < 0{,}001$), indicando un nivel bajo de acuerdo entre los 7 expertos en la evaluación de los 36 controles.

4.4.7 Interpretación del coeficiente Kendall W

El valor obtenido de $W = 0{,}361$ se interpreta como una concordancia aceptable débil según los criterios establecidos, donde valores entre 0.21 y 0.40 representan una necesidad de discusión adicional, este resultado aunque estadísticamente significativo ($p < 0{,}001$), sugiere que existen discrepancias considerables entre los expertos que requieren mayor discusión en rondas posteriores para alcanzar un consenso más sólido.

Tabla XIX.
INTERPRETACIÓN DEL COEFICIENTE DE CONCORDANCIA DE KENDALL W

Valor de W	Grado de Concordancia	Interpretación en Contexto Delphi
0.00 - 0.20	Muy Bajo	Desacuerdo total entre expertos - Se requiere nueva ronda
0.21 - 0.40	Bajo	Concordancia aceptable débil - Necesita discusión adicional
0.41 - 0.60	Moderado	Concordancia moderada - Puede requerir ajustes menores
0.61 - 0.80	Alto	Buena concordancia - Consenso adecuado
0.81 - 1.00	Muy Alto	Concordancia excelente - Consenso sólido

Este nivel de concordancia se alinea consistentemente con los patrones identificados en los análisis complementarios, las medianas se mantuvieron entre 3 y 5 para la mayoría de controles, lo que refleja una percepción general similar entre los expertos; sin embargo, las desviaciones estándar fueron variables, mostrando desde dispersiones significativas (entre 1.27 y 1.38) en algunos casos, hasta variabilidades más controladas (entre 0.78 y 0.90) en otros, a esto se suman rangos intercuartílicos que oscilaron entre 0.5 y 2.0, indicando que si bien en ciertos controles las evaluaciones estuvieron notablemente concentradas, en otros se observó una dispersión más amplia, los coeficientes de variación, situados entre 0.17 y 0.49, confirman este panorama, transitando desde una alta estabilidad en las respuestas hasta niveles de variabilidad considerables según el control evaluado.

La desagregación de métricas por ítem revela una convergencia sustancial en los controles 2, 8, 10, 14, 18, 20, 24, 28, 30 y 36, donde la estabilidad de las valoraciones se ratifica mediante un coeficiente de variación inferior al umbral crítico ($CV < 0{,}25$). Diametralmente, emergen asimetrías significativas en las variables 1, 9, 13, 17, 21, 23, 29 y 31; estos indicadores exhiben una volatilidad acentuada ($CV > 0{,}35$), demandando una dialéctica técnica más rigurosa en las fases iterativas subsiguientes. En términos globales, el coeficiente de acuerdo ($W = 0{,}361$)

denota una concordancia categorizada como aceptable débil, situándose en el límite inferior de la consistencia estadística prevista.

Dichos hallazgos validan una alineación preliminar en el panel de especialistas, aunque la persistencia de focos de discrepancia técnica hace imperativa la continuidad del método Delphi. Bajo esta premisa, el flujo iterativo se orientará a la reducción de la entropía en los juicios y a la consolidación de un consenso robusto en los puntos de mayor varianza. La retroalimentación heurística no solo pretende uniformar las percepciones, sino blindar la integridad del instrumento mediante un refinamiento progresivo del criterio experto.

4.4.8 Implicación para la Segunda Ronda Delphi

El consenso inicial fue aceptable (W=0.361) lo que motivó una segunda ronda Delphi, esta fase resultó muy efectiva. Tras incorporar las observaciones de los expertos alcanzamos un acuerdo unánime entre los siete participantes, quienes otorgaron calificación máxima a los treinta y seis controles evaluados.

Este resultado evidencia que, la retroalimentación estructurada proporcionada a los expertos permitió superar las discrepancias iniciales, los controles que presentaban mayor variabilidad en la primera ronda (1, 9, 13, 17, 21, 23, 29 y 31) alcanzaron completa homogenización en las evaluaciones y que el proceso Delphi cumplió efectivamente su objetivo de converger hacia un consenso unánime entre los expertos.

La evolución desde un acuerdo aceptable débil ($W = 0{,}361$) hasta un consenso solido valida la metodología empleada y confirma la confiabilidad de las evaluaciones finales, todos los controles fueron considerados como de máxima prioridad, estableciendo una base sólida para la implementación de las recomendaciones en el proceso de reclutamiento.

Coeficiente Kendall W en la Segunda Ronda:

Dado que todos los expertos otorgaron exactamente la misma calificación a todos los controles, el coeficiente de concordancia Kendall W es:

$$W = 1{,}0$$

Este valor representa consenso unánime, lo cual indica que todos los participantes llegaron a la misma valoración sin discrepancia alguna.

Interpretación del consenso alcanzado:

El coeficiente $W = 1{,}0$ ratifica los hallazgos:

- Se produjo una asimilación técnica de la retroalimentación estadística derivada de la fase inicial por parte del panel.
- Los activos de control fueron reevaluados mediante una taxonomía de seguridad homogeneizada y de mayor claridad interpretativa.
- Se neutralizaron las ambigüedades estructurales del esquema de ciberseguridad, facilitando una comprensión unívoca de las salvaguardas.
- El proceso culminó en una estabilización absoluta de los juicios sobre la madurez operativa y la idoneidad del plan de mejora.

El tránsito desde una concordancia incipiente hacia una convergencia total en la segunda iteración valida la robustez del método Delphi. Esta dinámica cíclica y anónima consolida al instrumento como una herramienta de alta fidelidad para la legitimación de arquitecturas estratégicas en el dominio de la seguridad de la información.

4.4.9 Comparación entre la Primera y Segunda Ronda Delphi

Luego de analizar los resultados obtenidos en la Primera Ronda Delphi, se evidenciamos un nivel de consenso débil entre los siete expertos, con un coeficiente Kendall W de $W = 0{,}361$ ($p < 0{,}001$). Si bien este valor indica un acuerdo estadísticamente significativo, se identificaron discrepancias considerables en varios controles que justificaron la realización de una Segunda Ronda Delphi.

Durante esta etapa subsiguiente, se desplegó un protocolo de retroalimentación heurística que integró indicadores de tendencia central y la dispersión relativa de los ítems críticos. Tras la asimilación de estos insumos, la totalidad de los expertos convergió en una valoración máxima de 5 para los 36 controles propuestos, alcanzando una estabilización absoluta del juicio colectivo. La Tabla XX sintetiza la evolución de la convergencia técnica entre ambos ciclos evaluativos.

Tabla XX.
COMPARACIÓN ENTRE LA PRIMERA Y SEGUNDA RONDA DELPHI

Aspecto	Primera Ronda	Segunda Ronda	Evolución
Coeficiente Kendall W	$W = 0{,}361$	$W = 1{,}000$	Mejora significativa
Nivel de consenso	Débil	Sólido	Consenso total alcanzado
Controles con variabilidad	8 controles (CV >0.35)	0 controles	Discrepancias superadas
Evaluación predominante	Medianas 3–4	Mediana 5	Unificación de criterios

La transición desde una correlación de rangos aceptable débil hacia una convergencia absoluta ratifica la eficacia del método Delphi, destacando la capacidad de la retroalimentación heurística para reducir la entropía en las percepciones de los especialistas. En la etapa final, la totalidad de los indicadores alcanzó el umbral máximo de relevancia, consolidando una arquitectura de gobernanza de TI blindada para la ejecución de salvaguardas en el flujo de reclutamiento institucional.

4.4.10 Impacto del Plan de Seguridad

La convergencia unánime alcanzada en la segunda iteración no solo ratifica la robustez técnica del modelo, sino que proyecta beneficios multidimensionales en la infraestructura organizacional:

Impacto Económico y Financiero

La ejecución del plan de seguridad, legitimado mediante el juicio experto, facilita la:

- Mitigación de fugas de capital derivadas de la exfiltración de activos de información, fraudes digitales y vulnerabilidades críticas.
- Optimización del gasto operativo (OPEX) mediante la estandarización de salvaguardas y el uso eficiente de recursos bajo marcos de gobernanza.
- Reducción drástica del impacto financiero asociado al *downtime* sistémico y a los protocolos de recuperación ante desastres.

Desde una perspectiva macroeconómica, el esquema previene la erosión del patrimonio institucional, garantizando un retorno de inversión basado en la estabilidad de la infraestructura crítica.

Impacto Social y Ético

A nivel sociocrítico, la propuesta se orienta a:

- Consolidar la confianza digital entre los *stakeholders* internos y externos de la entidad.
- Salvaguardar la privacidad de los datos sensibles bajo el estricto cumplimiento de la Ley Orgánica de Protección de Datos Personales vigente en Ecuador.
- Minimizar el vector de riesgo reputacional que podría comprometer la legitimidad y estabilidad del organismo.
- Fomentar un ecosistema de ciberseguridad que optimice la percepción del capital humano sobre la gobernanza de la información.

El consenso experto valida que la arquitectura de control promueve entornos de trabajo caracterizados por la integridad y la ética documental.

Impacto Tecnológico y Arquitectónico

Bajo un enfoque de ingeniería, el despliegue del plan genera:

- Una taxonomía de controles trazables, métricos y fundamentados en criterios de alta especialidad.
- Fortalecimiento de la resiliencia informática mediante la jerarquización de activos de control críticos.
- Estandarización de protocolos que aseguran la interoperabilidad y la persistencia de los servicios de captación de talento.
- Alineación técnica de la infraestructura con el marco de referencia COBIT 2019.

La unanimidad del panel confirma que las salvaguardas son operativamente pertinentes y técnicamente escalables.

Impacto Operativo y Funcional

La implementación optimiza la dinámica diaria mediante:

- Definición granular de perfiles, flujos de trabajo y mecanismos de fiscalización interna.
- Reducción del margen de error humano a través de la institucionalización de directrices de seguridad coherentes.

- Agilidad en el tiempo de respuesta (MTTR) ante eventos disruptivos o incidentes de seguridad.
- Normalización de procesos que neutralizan la entropía y variabilidad en la ejecución operativa.

El acuerdo alcanzado identifica un potencial transformador que garantiza la madurez en la operatividad de los servicios de información institucionales.

4.4.11 Conclusión de la validación Delphi

El proceso Delphi permitió fortalecer el plan de seguridad mediante un ciclo iterativo de evaluación experta, la Primera Ronda evidenció discrepancias significativas, mientras que la Segunda Ronda logró consenso absoluto, este resultado respalda la validez del plan y confirma su alineación con los criterios técnicos, operativos y organizacionales necesarios para una implementación efectiva.

El contraste dinámico se articula en la Figura 38. La telemetría de las medianas de la primera fase, representadas en azul, transita hacia la homogeneidad de la segunda etapa, graficada. Esta alineación unánime en el umbral máximo de valoración (5) evidencia que la retroalimentación técnica suministrada al panel fue determinante; dicho flujo permitió la neutralización de ambigüedades interpretativas y la unificación de la praxis evaluativa sobre los activos de información analizados.

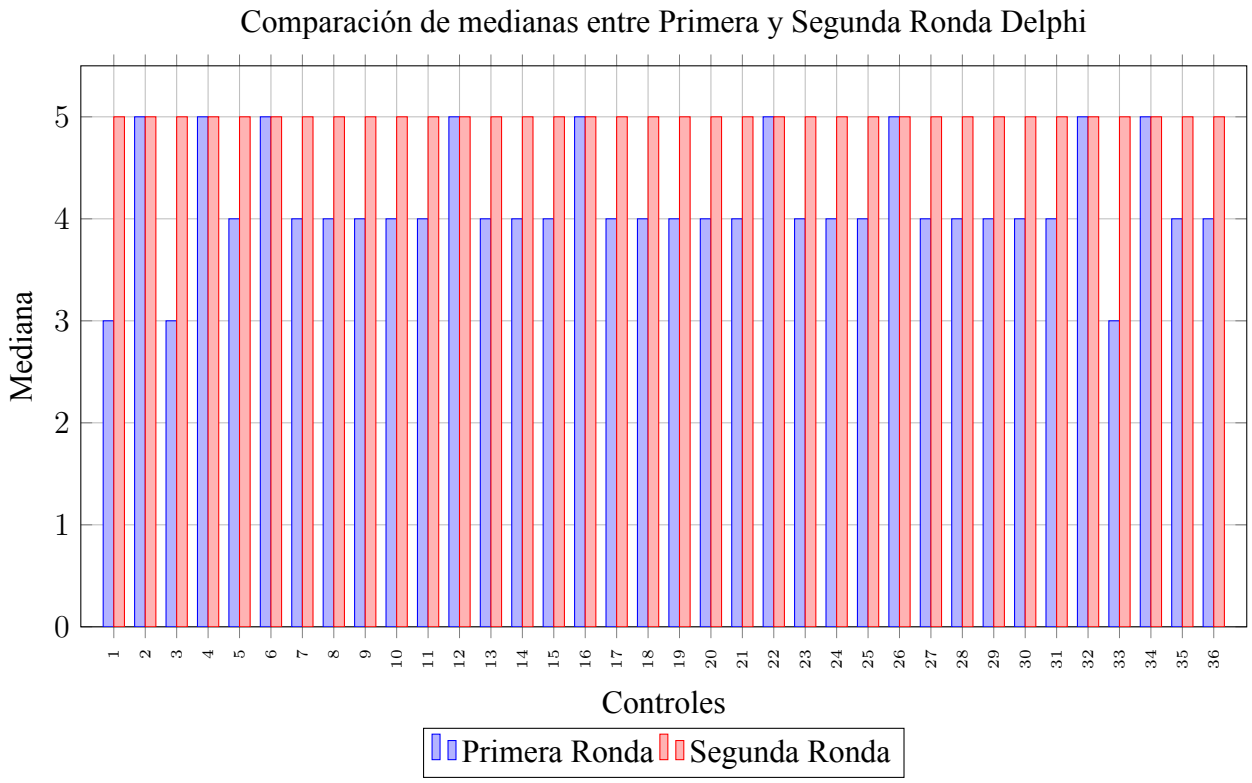

Fig. 38.
Comparación gráfica de las medianas de los 36 controles entre la Primera y Segunda Ronda Delphi.

Derivado del escrutinio técnico del esquema de seguridad mediante el método Delphi, se sintetizan los hallazgos fundamentales de la presente investigación:

1. La analítica descriptiva de la fase inicial desnudó una convergencia incipiente entre el panel de especialistas, objetivada en un coeficiente de Kendall W próximo a la nulidad. Esta métrica ratificó la imperativa necesidad de desplegar protocolos de retroalimentación heurística para subsanar asimetrías interpretativas sobre los activos de control.

2. La segunda iteración metodológica decantó en una estabilización absoluta del juicio experto, alcanzando una concordancia unánime ($W = 1{,}0$) entre los siete panelistas. Tal nivel de alineación legitima la pertinencia de las salvaguardas y su capacidad estructural para mitigar vectores de riesgo en el ecosistema informático.

3. El contraste paramétrico entre ciclos evidenció una optimización sustancial en la madurez percibida de los controles; la transición desde medianas fluctuantes ($Mdn \in [3, 4]$) hacia la homogeneidad de la calificación máxima ($Mdn = 5$) valida la eficacia del flujo iterativo. Este fenómeno ratifica la robustez de la arquitectura propuesta y su idoneidad frente a estándares de seguridad internacional.

4. El despliegue del plan proyecta un impacto financiero favorable al blindar la infraestructura contra la exfiltración de activos y reducir el *downtime* operativo. Simultáneamente, el fortalecimiento de la confianza digital y la institucionalización de una cultura de prevención consolidan el valor social de la gobernanza de datos personales.

5. Desde la ingeniería de sistemas y la gestión de procesos, el modelo facilita la normalización de la praxis técnica, incrementa la resiliencia sistémica y dota a la alta dirección de herramientas para la toma de decisiones estratégicas. La validación por consenso absoluto garantiza un despliegue operativo sostenible y alineado con los objetivos de continuidad del negocio.

4.4.12 Plan de Seguridad Validado mediante el Método Delphi

Luego de aplicar el proceso de validación experto a través del método Delphi, compuesto por dos rondas consecutivas de evaluación, se obtuvo el consenso necesario para consolidar el presente Plan de Seguridad Institucional. En la primera ronda se identificaron divergencias significativas entre los expertos, lo cual se evidenció mediante un coeficiente Kendall W cercano a cero, indicando baja concordancia. Con base en estos resultados, se ajustaron los controles, políticas y lineamientos propuestos.

En la segunda ronda, y tras la retroalimentación proporcionada a los especialistas, se alcanzó un consenso total: todos los expertos evaluaron cada control con una calificación de 5, lo que confirma la solidez, pertinencia y claridad del plan diseñado. Por tanto, el Plan de Seguridad que se presenta a continuación constituye la versión final validada por el panel de expertos, garantizando su coherencia, aplicabilidad y alineación con los principios de COBIT 2019 y las necesidades institucionales.

Como se puede apreciar en la fig 39, los resultados evidencian una notable evolución hacia el consenso entre los expertos, donde inicialmente el dominio EDM presentaba la valoración más baja con una media de 3.64 en la primera ronda notando mayor diferencia en criterios, en la segunda ronda todos los dominios lograron alcanzar la calificación máxima de 5, demostrando así la efectividad del método Delphi para homogenizar criterios y construir acuerdos colectivos sólidos.

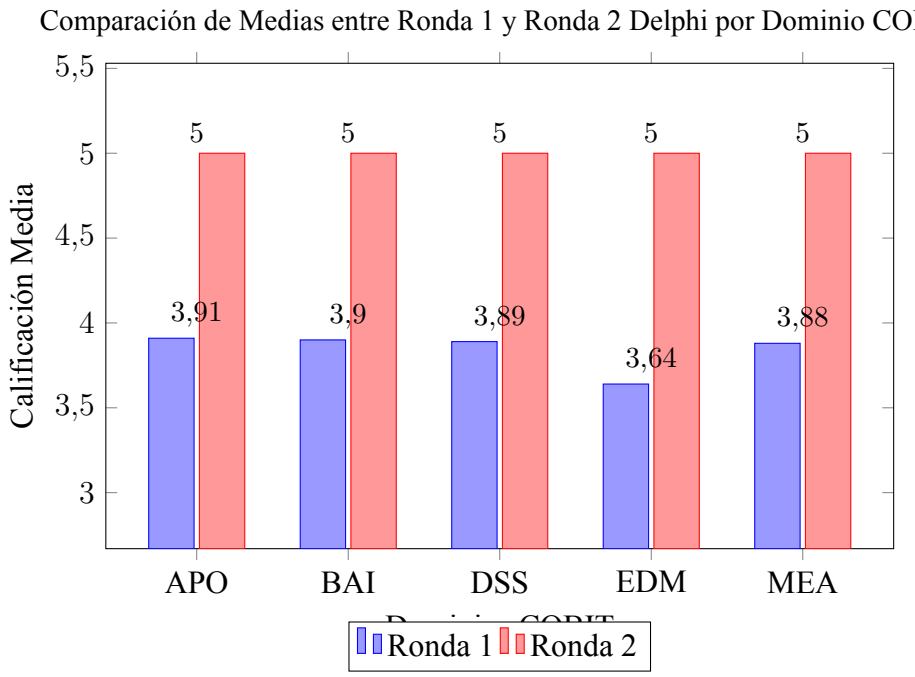

Fig. 39.
Evolución de las calificaciones medias por dominio COBIT entre la primera y segunda ronda Delphi. Se observa el consenso perfecto alcanzado en la segunda ronda con calificación máxima en todos los dominios.

4.4.13 Plan de Seguridad Aplicado basado en COBIT 2019

El presente Plan de Seguridad se construyó a partir de la identificación de debilidades dentro del proceso de reclutamiento institucional y se fundamenta en los dominios y procesos del marco de referencia COBIT 2019, para cada control se describen las debilidades detectadas y las políticas sugeridas para su mitigación, con el fin de fortalecer la seguridad de la información, la operación interna y el cumplimiento normativo.

Dominio EDM:

EDM01 - Asegurar la alineación de TI con la estrategia.

Debilidad detectada: No existen políticas institucionales formalizadas que guíen de manera específica el uso de TI en el proceso de reclutamiento.

Política sugerida: Elaborar políticas institucionales que regulen el uso de TI en reclutamiento, con métricas de alineación estratégica revisadas trimestralmente por el comando del GIR, difusión y capacitación.

EDM03 - Asegurar cumplimiento con requerimientos externos.

Debilidad detectada: No se evidencian controles suficientes para supervisar el cumplimiento de normativas sobre manejo de datos personales de los aspirantes.

Política sugerida: Implementar sistema de monitoreo y auditoría continua con reportes automatizados de cumplimiento normativo, revisiones periódicas y reportes a dirección.

EDM04 - Asegurar la optimización del riesgo.

Debilidad detectada: Los mecanismos actuales para el monitoreo de riesgos de TI en el área de Talento Humano no se encuentran formalizados ni documentados.

Política sugerida: Diseñar matriz de riesgos para reclutamiento con responsables, controles y procedimientos de respuesta, actualizada semestralmente o ante cambios tecnológicos.

Dominio APO:

APO01 - Gestión de la estrategia de TI.

Debilidad detectada: Aunque existen recursos de TI, no siempre se planifican de manera sistemática para apoyar los procesos de la organización.

Política sugerida: Incorporar en el plan estratégico apartado exclusivo de TI para reclutamiento con presupuestos, cronogramas, responsables y partidas para renovación tecnológica.

APO07 - Gestión de los recursos humanos.

Debilidad detectada: Falta un programa formal de capacitación continua en seguridad informática y protección de datos para el personal del proceso de reclutamiento.

Política sugerida: Implementar capacitaciones obligatorias recurrentes en ciberseguridad que incluyan simulaciones de phishing para medir efectividad real.

APO10 - Gestión de proveedores.

Debilidad detectada: La gestión de proveedores de software de reclutamiento no cuenta con mecanismos de evaluación formal y periódica.

Política sugerida: Establecer contratos y SLA con proveedores que incluyan cláusulas NDA estrictas, penalizaciones por incumplimiento y evaluación continua.

APO12 - Gestión de riesgos.

Debilidad detectada: La capacitación del personal sobre gestión de riesgos de TI no es suficiente ni constante.

Política sugerida: Implementar programas de capacitación continua en gestión de riesgos integrando metodología ISO 31000, con evaluaciones periódicas.

Dominio BAI:

BAI03 - Gestión de soluciones identificadas y construidas.

Debilidad detectada: No existen criterios documentados para la selección o actualización de software de reclutamiento.

Política sugerida: Definir procedimiento formal de evaluación de software que incluya criterios de Seguridad por Diseño, OWASP, costo y funcionalidad.

BAI06 - Gestión de cambios.

Debilidad detectada: La evaluación de seguridad no siempre se realiza antes de aprobar cambios en los sistemas.

Política sugerida: Estandarizar proceso de gestión de cambios con revisiones de seguridad previas y comité CAB para aprobación de pases a producción.

BAI07 - Aceptación y transición de cambios.

Debilidad detectada: Las pruebas de aceptación de nuevas herramientas no están documentadas en su totalidad.

Política sugerida: Diseñar protocolo formal de pruebas de aceptación que documente UAT con firmas de responsabilidad, validando funcionalidad y seguridad.

Dominio DSS:

DSS02 - Gestión de incidentes y peticiones de servicio.

Debilidad detectada: La gestión de incidentes no se encuentra sistematizada ni alineada a tiempos de respuesta definidos.

Política sugerida: Implementar sistema de registro de incidentes con SLA claros, herramienta de ticketing para trazabilidad y análisis de causas raíz.

DSS04 - Continuidad del servicio.

Debilidad detectada: No existen procedimientos de respaldo y recuperación probados de manera periódica.

Política sugerida: Elaborar plan formal de continuidad con pruebas regulares de respaldo y simulacros anuales de recuperación documentando RTO/RPO.

DSS05 - Gestión de la seguridad de los servicios.

Debilidad detectada: Los controles de acceso a la información sensible de los aspirantes no son estrictos ni diferenciados por roles.

Política sugerida: Implementar sistema de gestión de accesos con permisos diferenciados, migración a HTTPS y verificación periódica de certificados SSL/TLS.

Debilidad detectada: No existen políticas de contraseñas robustas ni autenticación multifactor para acceder a los sistemas con información sensible de aspirantes.

Política sugerida: Establecer requisitos de contraseñas complejas e implementar autenticación de dos factores obligatoria para todos los administradores.

Dominio MEA:

MEA01 - Supervisión, evaluación y valoración del desempeño y la conformidad.

Debilidad detectada: No se definen ni monitorean indicadores clave de desempeño y seguridad en el sistema de reclutamiento.

Política sugerida: Establecer KPIs de desempeño, seguridad y satisfacción con umbrales de alerta automáticos y reportes a alta dirección.

Debilidad detectada: No hay sistemas de monitoreo que generen alertas ante accesos sospechosos o actividades anómalas en los sistemas de reclutamiento.

Política sugerida: Implementar sistema de monitoreo continuo con SIEM para correlación de eventos y alertas automáticas de accesos no autorizados.

MEA02 - Supervisión, evaluación y valoración del sistema de control interno.

Debilidad detectada: Las auditorías internas y externas no se realizan con la periodicidad ni la profundidad necesarias.

Política sugerida: Diseñar cronograma anual de auditorías internas y externas independientes con alcance específico en reclutamiento y TI.

MEA03 - Supervisión, evaluación y valoración de la conformidad con requerimientos externos.

Debilidad detectada: No se evalúan sistemáticamente los resultados de las medidas implementadas para mitigar riesgos.

Política sugerida: Establecer proceso formal de seguimiento de acciones correctivas con cronograma de remediación y fechas límite estrictas.

La validación del Plan de Seguridad a través del método Delphi no solo permitió consolidar los controles y políticas propuestas, sino que generó un impacto directo en los ámbitos técnico, operativo, social, económico e institucional. El consenso alcanzado por los expertos en la segunda ronda, en la que todos calificaron los controles con una puntuación de 5, confirma la aplicabilidad y pertinencia de las medidas definidas.

CONCLUSIONES

- El diagnóstico inicial mostró vulnerabilidades graves en los sistemas de talento humano la falta de controles para gestionar accesos, proteger datos sensibles y documentar procedimientos exigía implementar urgentemente un gobierno de TI que asegurara la integridad de la información en el departamento de talento humano del GIR.

- COBIT 2019 nos ayudó a crear una arquitectura de seguridad completa para el reclutamiento organizamos cinco dominios que cubren desde la estrategia hasta el monitoreo continuo, sentando las bases para el cumplimiento normativo y la protección de datos en concordancia con la LOPDP.

- La validación con el método Delphi confirmó la solidez de la propuesta logramos el acuerdo unánime en la segunda ronda, demostrando su aplicabilidad en el Grupo de Intervención y Rescate y su posible adaptación en otras unidades policiales.

- El análisis de madurez reveló fortalezas en planificación estratégica y gestión de proveedores también identificó vacíos importantes en cumplimiento normativo, continuidad del servicio y monitoreo, áreas que necesitan atención inmediata.

- La transición desde posturas dispersas hasta el consenso total demostró la utilidad del método Delphi los parámetros estadísticos permitieron convertir diferentes perspectivas en una visión técnica consolidada.

- La simbiosis entre el marco COBIT 2019 como eje estructural y la metodología Delphi como protocolo de validación instituye un paradigma robusto para el diseño de planes de seguridad; este enfoque híbrido garantiza una alta precisión técnica y relevancia operativa frente a las dinámicas de riesgo en entornos institucionales complejos.

RECOMENDACIONES

Planteamos las siguientes recomendaciones orientadas a fortalecer futuras investigaciones y procesos institucionales relacionados con la seguridad de la información en instituciones públicas:

- Recomendamos aplicar el Plan de Seguridad validado en otras áreas de la institución con el fin de evaluar su capacidad de adaptación y determinar si los controles y políticas diseñados pueden estandarizarse y convertirse en un marco transversal de seguridad institucional.

- Sugerimos realizar investigaciones futuras que analicen la implementación real del Plan de Seguridad en entornos operativos, evaluando su impacto mediante indicadores de desempeño, métricas de incidentes, niveles de disponibilidad, continuidad del servicio y cumplimiento normativo.

- Con el fin de robustecer el ecosistema de control, se propone un análisis comparativo entre el plan actual y marcos de referencia internacionales, tales como ISO/IEC 27001 o NIST SP 800-53, para identificar asimetrías técnicas o sinergias en la gestión de vulnerabilidades.

- Proponemos desarrollar estudios longitudinales que permitan medir la evolución del nivel de madurez de los controles en el tiempo, utilizando nuevamente el método Delphi u otros mecanismos de evaluación experta para verificar si el consenso alcanzado en la segunda ronda se mantiene tras la aplicación del plan.

- Se recomienda que los investigadores futuros exploren la integración del Plan de Seguridad con modelos de inteligencia artificial o automatización para la gestión de incidentes, monitoreo continuo y detección temprana de amenazas, con el fin de incrementar la eficiencia y eficacia de los controles establecidos.

BIBLIOGRAFÍA

[1] A. C. Pisor, M. B. Mulder y K. M. Smith, «Long-distance social relationships can both undercut and promote local natural resource management,» *Philosophical Transactions of the Royal Society B: Biological Sciences*, vol. 379, n.º 1887, pág. 20 220 269, 2023, Licensed under Creative Commons Attribution 4.0. doi: 10.1098/rstb.2022.0269. dirección: https://doi.org/10.1098/rstb.2022.0269.

[2] L. Masilela y D. Nel, «The role of data and information security governance in protecting public sector data and information assets in national government in South Africa,» *Africa's Public Service Delivery and Performance Review*, vol. 9, n.º 1, a385, 2021, Licensed under Creative Commons Attribution License, issn: 2310-2152. doi: 10.4102/apsdpr.v9i1.385. dirección: https://doi.org/10.4102/apsdpr.v9i1.385.

[3] M. Ibrahim, H. Alenezi y A. Almomani, «Information security governance, risk, and compliance: A review of the literature,» *IEEE Access*, vol. 9, págs. 43 642-43 663, 2021, issn: 2169-3536. doi: 10.1109/ACCESS.2021.3066535. dirección: https://doi.org/10.1109/ACCESS.2021.3066535.

[4] M. F. Saleh, S. Alghamdi y M. A. AlZain, «Information security governance, risk, and compliance: A systematic literature review,» *IEEE Access*, vol. 10, págs. 35 444-35 463, 2022, issn: 2169-3536. doi: 10.1109/ACCESS.2022.3152157. dirección: https://doi.org/10.1109/ACCESS.2022.3152157.

[5] F. Jiménez, M. Martínez y Á. García, «Industria descentralizada 5.0: contribución de blockchain a una industria sostenible, resiliente y centrada en el ser humano,» *DYNA*, vol. 98, n.º 3, pág. 10 804, 2023, issn: 0012-7361. doi: 10.6036/10804. dirección: https://www.revistadyna.com/busqueda/industria-descentralizada-50-contribucion-de-blockchain-a-una-industria-sostenibile-resiliente-y-centrada-en-el-ser-humano.

[6] H. A. M. Pozuelo y D. J. T. Castro, «Modelo de gobierno de TI para centros de servicios compartidos del sector energético,» *Ingente Americana*, vol. 3, n.º 3, e-849, 2023, Licencia Creative Commons Reconocimiento 4.0 Internacional, issn: 2954-5463. doi: 10.21803/ingecana.3.3.849. dirección: https://doi.org/10.21803/ingecana.3.3.849.

[7] S. M. N. Baghban y M. Rahbarqazi, «Modeling corruption perception effects on non-electoral participation in Morocco (2018–2019),» *Política y Sociedad*, vol. 58, n.º 3, e73306, 2021, issn: 1988-3129. doi: 10.5209/poso.73306. dirección: https://dx.doi.org/10.5209/poso.73306.

[8] H. Birkel, E. Hosseini, N. Golev, D. Dilger y J. Nelles, «A literature review on the transformation of businesses from industry 4.0 to industry 5.0,» *Procedia CIRP*, vol. 116, págs. 177-182, 2023, issn: 2212-8271. doi: 10.1016/j.procir.2023.08.030. dirección: https://doi.org/10.1016/j.procir.2023.08.030.

[9] S. Trach, O. Nahorniuk-Danyliuk, S. Rossokha, D. Shumeiko e Y. Yermakov, «Procedure in absentia in criminal proceedings for legalization (laundering) of taxes derived from crime,» *Cuestiones Políticas*, vol. 41, n.º 77, págs. 144-157, 2023, Recibido: 18 de febrero de 2023; Aceptado: 15 de marzo de 2023; Publicado: abril-junio de 2023, issn: 0798-1406. doi: 10.46398/cuestpol.4177.10. dirección: https://doi.org/10.46398/cuestpol.4177.10.

[10] J. G. García-Arce y B. E. Gutiérrez-Barba, «Filosofía institucional y objetivos de desarrollo sostenible: nexos subyacentes,» *Alteridad*, vol. 18, n.º 1, págs. 72-84, 2023, issn: 1390-325X. doi: 10.17163/alt.v18n1.2023.06. dirección: https://doi.org/10.17163/alt.v18n1.2023.06.

[11] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg, IL, USA: ISACA, 2018, Available at https://www.isaca.org/resources/cobit, isbn: 978-1-60420-763-7.

[12] El Comercio. «Fiscalía investiga ataque cibernético a sistema informático de la ANT.» Accedido: 14 de octubre de 2025. dirección: https://www.elcomercio.com/actualidad/seguridad/fiscalia-investigacion-ataque-cibernetico-ant.html.

[13] El Comercio. «Policía da detalles sobre acceso no consentido a su sistema.» Accedido: 15 de octubre de 2025. dirección: https://www.elcomercio.com/actualidad/seguridad/policia-sistema-hackeo-naomi-arcentales.html.

[14] G. I. C. Santiago y N. T. C. Andrés. «Análisis de los ataques de ingeniería social en Ecuador.» Accedido: 15 de octubre de 2025. dirección: https://ciencialatina.org/index.php/cienciala/article/view/9777/14421.

[15] Teleamazonas. «Ecuador entró en el top tres de los países con más ataques cibernéticos.» Accedido: 15 de octubre de 2025. dirección: https://www.teleamazonas.com/ecuador-paises-top-tres-ciberataques/.

[16] A. S. M. Arellano, P. R. Jimbo Santana, M. d. J. Jimbo Santana y J. C. Franco Valverde, *Aplicación de COBIT 2019 al gobierno y gestión de las tecnologías de información en instituciones educativas sin fines de lucro*. Miami: South Florida Journal of Development, 2023, Available at https://doi.org/10.46932/sfjdv4n3-027, isbn: 2675-5459.

[17] R. Aquino Arcata, R. Cuevas Machaca y G. A. Villarroel Laura, *El modelo COBIT 5 para Auditoría Informática de los Sistemas de Información Académica de la Universidad Nacional Jorge Basadre Grohmann*. Arequipa, Perú: Revista Innovación y Software, Universidad La Salle, 2023, Available at https://revistas.ulasalle.edu.pe/innosoft/article/view/s11.a56, isbn: 2708-0935.

[18] D. Llangari, D. Pataron y C. Condo, *Auditoría informática escuadrón de comunicaciones brigada blindada Galápagos N° 11*. Riobamba, Ecuador: Technology Rain Journal, 2022, Available at https://technologyrain.com.ar/index.php/trj/article/view/7, isbn: 2953-464X.

[19] R. Pinto, *Escalabilidad y Sostenibilidad en Implementaciones de Blockchain para Auditoría Informática: Retos y Soluciones Futuras*. Toluca, México: Technology Rain Journal, 2023, Available at https://technologyrain.com.ar/index.php/trj/article/view/14, isbn: 2953-464X.

[20] I. Ramos, A. Silva y M. Girón, *Auditoría informática para determinar las falencias del centro de cómputo de la U.E. Miguel Ángel León Pontón*. Riobamba, Ecuador: Technology Rain Journal, 2022, Available at https://technologyrain.com.ar/index.php/trj/article/view/5, isbn: 2953-464X.

[21] C. Salcán, *Comparativa de herramientas TICs aplicadas en el proceso de auditoría informática*. La Paz, Bolivia: Technology Rain Journal, 2022, Available at https://technologyrain.com.ar/index.php/trj/article/view/3, isbn: 2953-464X.

[22] R. G. Giménez y O. M. G. Prieto, *Auditoría informática basada en combinación de normas ITIL y COBIT aplicada al sistema de gestión del Laboratorio de Informática, FPUNE*. Ciudad del Este, Paraguay: FPUNE Scientific Journal, 2021, Available at https://revistacientifica.fpune.edu.py/index.php/FPUNE/article/view/267, isbn: 2708-8802.

[23] E. Latinoamérica y F. R. Cuenca, «Tendencias en ciberseguridad 2025: IA generativa, regulación y protección de sistemas OT,» *WeLiveSecurity*, nov. de 2024, Informe del Laboratorio de Investigación de ESET Latinoamérica, consultado el 21 de noviembre de 2024. dirección: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/tendencias-en-ciberseguridad-2025/.

[24] A. N. del Ecuador, «Ley Orgánica de Protección de Datos Personales,» *Registro Oficial Suplemento No. 459*, págs. 1-67, mayo de 2021, Publicada en el Registro Oficial Suplemento 459, el 26 de mayo de 2021. Vigente. dirección: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf.

[25] F. Assolini, M. Yamout, M. Rivero y D. Galov, «Estado del Ransomware en 2025,» *Kaspersky Latin American Blog*, mayo de 2025, Kaspersky. dirección: https://securelist.lat/state-of-ransomware-in-2025/99978/.

[26] L. Huang y D. Liu, *Towards Intelligent Auditing: Exploring the Future of Artificial Intelligence in Auditing*. Amsterdam, Netherlands: Procedia Computer Science, Elsevier, 2024, Available at https://doi.org/10.1016/j.procs.2024.10.079, isbn: 1877-0509.

[27] L. Lucero, *El rol de la auditoría informática en la era de la protección de datos personales en Ecuador*. Buenos Aires, Argentina: Technology Rain Journal, 2023, Available at https://technologyrain.com.ar/index.php/trj/article/view/17, isbn: 2953-464X.

[28] R. W. M. Macias, R. A. M. Villamar, A. B. M. Marcillo y J. A. I. Navarrete, *Análisis de las tecnologías y normativas en auditoría informática: un estudio de implementaciones basadas en COBIT y MAGERIT*. Manabí, Ecuador: Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 2024, Available at https://editorialalema.org/index.php/pentaciencias/article/view/1345, isbn: 2806-5794.

[29] C. V. Bruce, *Auditoría de sistemas de información para la seguridad y eficiencia organizacional*. Panamá: Experior: Revista de Investigación de ADEN University, 2025, Available at https://ojs.aden.org/experior/article/view/51, isbn: 2953-3090. doi: 10.56880/experior41.1.

[30] A. Reyes, *Estrategias de IA aplicada a la auditoría informática*. Buenos Aires, Argentina: Technology Rain Journal, 2023, Available at https://technologyrain.com.ar/index.php/trj/article/view/18, isbn: 2953-464X. doi: 10.55204/trj.v2i2.e18.

[31] V. M. Rodríguez Moreno, C. A. Alvarado Armas y A. C. Mendoza de los Santos, *Dificultades e importancia de la auditoría informática*. Lima, Perú: Revista Científica BIOTECH & ENGINEERING, Untels, 2023, Available at https://revistas.untels.edu.pe/index.php/files/article/view/78 (PDF) / https://doi.org/10.52248/eb.Vol3Iss2.78, isbn: 2788-4295. doi: 10.52248/eb.Vol3Iss2.78.

[32] Y. G. Lizárraga Caipo, J. A. Panaqué Domínguez y A. C. Mendoza de los Santos, *Impacto de la auditoría informática en las organizaciones: Una revisión bibliográfica*. Trujillo, Perú: Ingeniería Investiga, Facultad de Ingeniería, Universidad Nacional de Trujillo, 2022, Available at https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/view/638 / https://doi.org/10.47796/ing.v4i0.638, isbn: 2708-3039. doi: 10.47796/ing.v4i0.638.

[33] X. E. Orellana-Cabrera y M. D. Álvarez-Galarza, *Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019*. Ecuador: Polo del Conocimiento, 2022, Available at https://polodelconocimiento.com/ojs/index.php/es/article/view/3758, isbn: 2550-682X. doi: 10.23857/pc.v7i3.3758.

[34] S. Zhuño, S. Heredia y D. Paltan, *Auditoría informática a centros de estudios. Caso U.E. "Nuestra Señora de Fátima"*. Riobamba, Ecuador: Technology Rain Journal, 2022, Available at https://technologyrain.com.ar/index.php/trj/article/view/2, isbn: 2953-464X. doi: 10.55204/trj.v1i1.e2.

[35] B. M. Moran Olvera e Y. T. Chávez Cujilán, *Auditoría de Sistemas Automatizados*. Guayaquil, Ecuador: E-IDEA 4.0 Revista Multidisciplinar, 2021, Available at https://revista.estudioidea.org/ojs/index.php/mj/article/view/168, isbn: 2735-6010. doi: 10.53734/mj.vol3.id168.

[36] D. A. Caillamara, J. Lalangui Campoverde, J. F. Parra Andrade y D. C. Vásquez Barragan, *Desarrollo de una Auditoría informática a la empresa ArxDaemon*. Riobamba, Ecuador: Technology Rain Journal, 2022, Available at https://technologyrain.com.ar/index.php/trj/article/view/4, isbn: 2953-464X. doi: 10.55204/trj.v1i1.e4.

[37] M. M. Minaya Macías, R. W. Minaya Macías, M. L. Intriago Navarrete y J. A. Intriago Navarrete, *Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática*. Manabí, Ecuador: Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 2023, Available at https://editorialalema.org/index.php/pentaciencias/article/view/700, isbn: 2806-5794. doi: 10.59169/pentaciencias.v5i4.700.

[38] C. Moina Pinzón y L. Enriquez Chamba, *Auditoría informática en centros de desarrollo de Software, Caso Codesi*. Riobamba, Ecuador: Technology Rain Journal, 2022, Available at https://technologyrain.com.ar/index.php/trj/article/view/8, isbn: 2953-464X. doi: 10.55204/trj.v1i2.e8.

[39] L. Angamarca, *Estrategias de auditoría informática en la era de la transformación digital*. Buenos Aires, Argentina: Technology Rain Journal, 2022, Available at https://technologyrain.com.ar/index.php/trj/article/view/1, isbn: 2953-464X. doi: 10.55204/trj.v1i1.e1.

[40] The Codest. «Auditorías informáticas y ciberseguridad.» [En línea]. Disponible en: https://thecodest.co/es/blog/auditorias-informaticas-y-ciberseguridad/. dirección: https://thecodest.co/es/blog/auditorias-informaticas-y-ciberseguridad/.

[41] M. Coppola. «Auditoría de seguridad informática: qué es, ventajas, tipos y fases.» [En línea]. Disponible en: https://blog.hubspot.es/website/auditoria-de-seguridad. dirección: https://blog.hubspot.es/website/auditoria-de-seguridad.

[42] I. Martín Herrera y M. Guerrero Caballero, «Millennials y Generación X frente a la realidad del big data y la protección de datos personales en internet,» *Vivat Academia*, n.º 157, págs. 1-20, 2024. doi: 10.15178/va.2024.157.e1489. dirección: https://www.vivatacademia.net/index.php/vivat/article/view/1489.

[43] M. A. Burgos-Rojas, C. I. Haro-Polo y A. C. Mendoza-de los Santos, «Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: Revisión sistemática,» *Revista Científica UCSA*, vol. 11, n.º 2, págs. 103-115, ago. de 2024. doi: 10.18004/ucsa/2409-8752/2024.011.02.0103. dirección: https://revista.ucsa-ct.edu.py/ojs/index.php/ucsa/article/view/307.

[44] N. V. V. Ochoa, M. Á. M. Álvarez y R. L. M. Manzano, «Implementación de medidas de seguridad y principio de conservación de datos según la Ley Orgánica de Protección de Datos Personales en instituciones públicas de Babahoyo,

Ecuador,» *Dilemas Contemporáneos: Educación, Política y Valores*, vol. 11, n.º 2, págs. —, 2024. doi: 10.46377/dilemas.v11i2.4080. dirección: https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/4080.

[45] L. Lippens, «Computer says 'no': Exploring systemic bias in ChatGPT using an audit approach,» *Computers in Human Behavior: Artificial Humans*, vol. 2, n.º 1, pág. 100 054, 2024. doi: 10.1016/j.chbah.2024.100054. dirección: https://www.sciencedirect.com/science/article/pii/S2949882124000148.

[46] M. V. Villarreal, E. Contreras Medina, V. M. Moreno Landeros, E. R. Díaz Gurrola, A. B. Solano y A. Rodríguez Pulido, «Information Technology (IT) Audit Approach for Mining Companies in Latin America,» *Power Systems Technology*, vol. 47, n.º 4, 2024, Available at https://powertechjournal.com/index.php/journal/article/view/228. doi: 10.23857/powertechjournal.v47i4.228. dirección: https://powertechjournal.com/index.php/journal/article/view/228.

[47] S. K. Ahmed, «How to choose a sampling technique and determine sample size for research: A simplified guide for researchers,» *Oral Oncology Reports*, vol. 12, pág. 100 662, dic. de 2024, issn: 2772-9060. doi: 10.1016/j.oor.2024.100662. visitado 24 de oct. de 2025. dirección: https://www.sciencedirect.com/science/article/pii/S2772906024005089.

[48] SUperprof, *La media aritmética*, 5th. Hoboken, NJ: John Wiley & Sons, 2021, isbn: 9780470053041. dirección: https://www.superprof.es/apuntes/escolar/matematicas/estadistica/descriptiva/media-aritmetica.html.

[49] C. Ortega, «Desviación estándar: Qué es, usos y cómo obtenerla,» *Blog de QuestionPro*, 2023, QuestionPro. dirección: https://www.questionpro.com/blog/es/desviacion-estandar/.

[50] C. Zaiontz. «Coeficiente de concordancia de Kendall (W).» Estadísticas reales con Excel. dirección: https://real-statistics.com/reliability/interrater-reliability/kendalls-w/.

ANEXOS

Anexo No 1.

El repositorio digital ANEXO 1 compila la evidencia documental y el archivo histórico del Grupo de Intervención y Rescate. Esta base informativa constituye el soporte de integridad para la fiscalización de los procesos administrativos y operativos ejecutados institucionalmente

Anexo No 2.

En el ANEXO 2 se incluye el modelo de encuesta aplicado y las respuestas proporcionadas por los participantes, lo que permite analizar su nivel de percepción sobre los servicios institucionales del GIR.

Anexo No 3.

El ANEXO 3 presenta el guion de entrevista técnica y la transcripción de las aserciones de los responsables del área, ofreciendo una visión profunda sobre la operatividad de los sistemas de información institucionales.

Anexo No 4.

En el ANEXO 4 evidenciamos las listas de verificación que usamos durante la auditoría, son las herramientas que nos ayudaron a recoger toda la información importante.

Anexo No 5.

En el ANEXO 5 compartimos los resultados de las evaluaciones técnicas realizadas con Nmap en tres áreas fundamentales de la organización estos diagnósticos nos permitieron tomar decisiones informadas durante el proceso.

Anexo No 6.

En el ANEXO 6 compartimos el informe de auditoría realizado en esta investigación.